Cryptography

Module 20

Cryptography

Cryptography is the study and art of hiding meaningful information in an unreadable format.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv10 Module 20 Cryptography

Lab Objectives

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption
- Perform cryptanalysis

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 110 Minutes

Overview of Cryptography

"Cryptography" comes from the Greek words ***kryptos***, meaning "concealed, hidden, veiled, secret, or mysterious," and ***graphia***, "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption**: Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption**: Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Encrypt the Information using Various Cryptography Tools	√	√	√
	1.1 Calculate One-way Hashes using HashCalc	√		√
	1.2 Calculate MD5 Hashes using MD5 Calculator		√	√
	1.3 Calculate MD5 Hashes using HashMyFiles		√	√
	1.4 Perform File and Text Message Encryption using CryptoForge	√		√

	1.5 Perform File Encryption using Advanced Encryption Package		√	
	1.6 Encrypt and Decrypt Data using BCTextEncoder		√	√
2	Create a Self-Signed Certificate	√		√
	2.1 Create and Use Self-signed Certificates	√		√
3	Perform Email Encryption		√	√
	3.1 Perform Email Encryption using Rmail		√	√
4	Perform Disk Encryption	√	√	√
	4.1 Perform Disk Encryption using VeraCrypt	√		√
	4.2 Perform Disk Encryption using BitLocker Drive Encryption		√	√
	4.3 Perform Disk Encryption using Rohos Disk Encryption		√	√
5	Perform Cryptanalysis using Various Cryptanalysis Tools		√	√
	5.1 Perform Cryptanalysis using CrypTool		√	√
	5.2 Perform Cryptanalysis using AlphaPeeler		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Lab 1

Encrypt the Information using Various Cryptography Tools

Cryptography is used to encrypt sensitive data to protect it from unauthorized access by any party other than the person for whom it is intended.

ICON KEY

- 📁 Valuable information
- ✎ Test your knowledge
- 💻 Web exercise
- 📖 Workbook review

Lab Scenario

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system.

📁 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography**

Lab Objectives

- Calculate one-way hashes using HashCalc
- Calculate MD5 hashes using MD5 Calculator
- Calculate MD5 hashes using HashMyFiles
- Perform file and text message encryption using CryptoForge
- Perform file encryption using advanced encryption package
- Encrypt and decrypt data using BCTextEncoder

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection

- Administrator privileges to run the tools
- HashCalc located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc**
- MD5 Calculator located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator**
- HashMyFiles located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles**
- CryptoForge located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**
- Advanced Encryption Package located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**
- BCTextEncoder located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 35 Minutes

Overview of Cryptography Tools

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

Lab Tasks

TASK 1

Calculate One-way Hashes using HashCalc

Here, we will use the HashCalc tool to calculate one-way hashes.

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

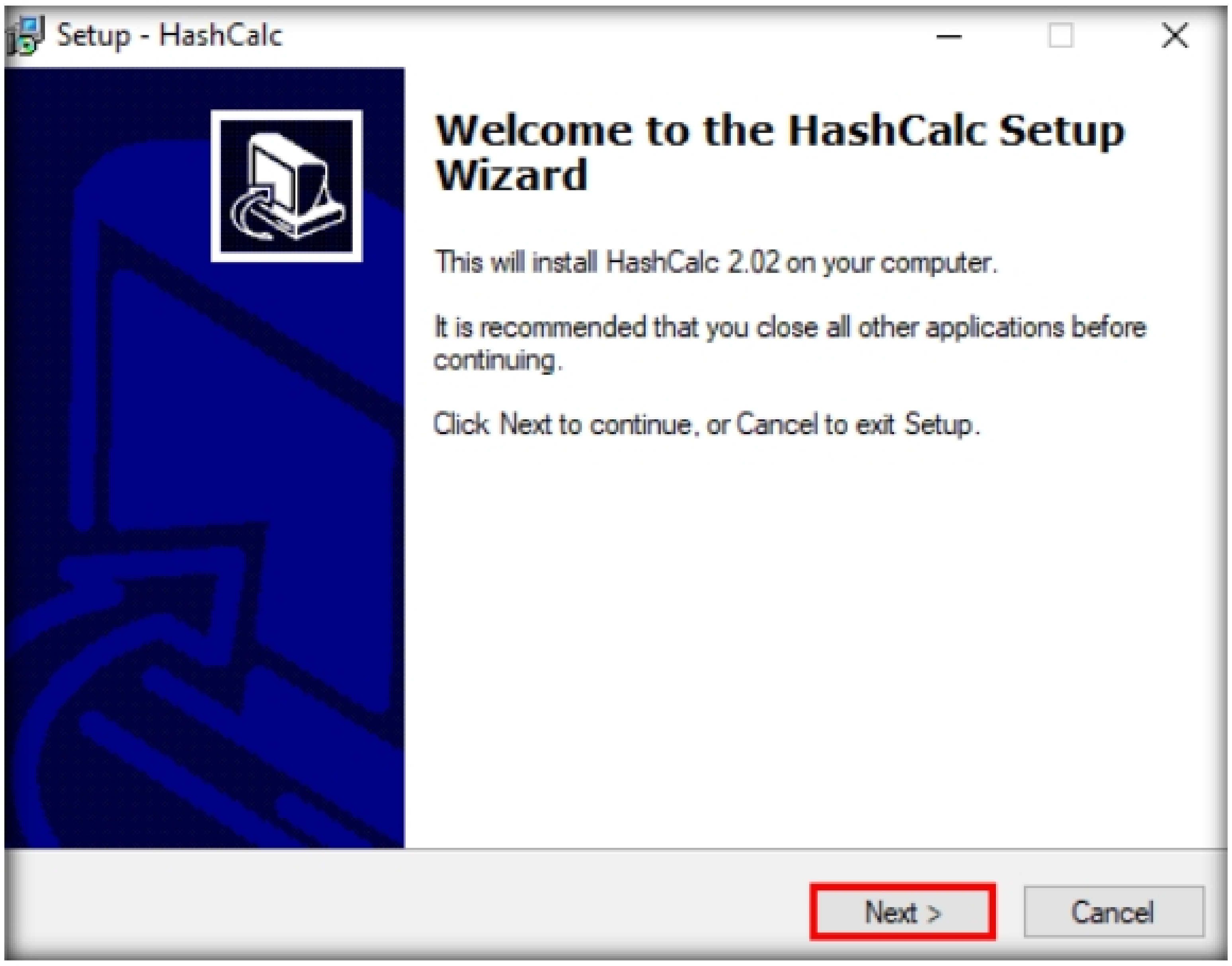
Install & Launch HashCalc Tool

2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc** and double click **setup.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **Setup - HashCalc** window appears, click **Next**.

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest (One-way Hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.


Welcome to the HashCalc Setup Wizard

This will install HashCalc 2.02 on your computer.

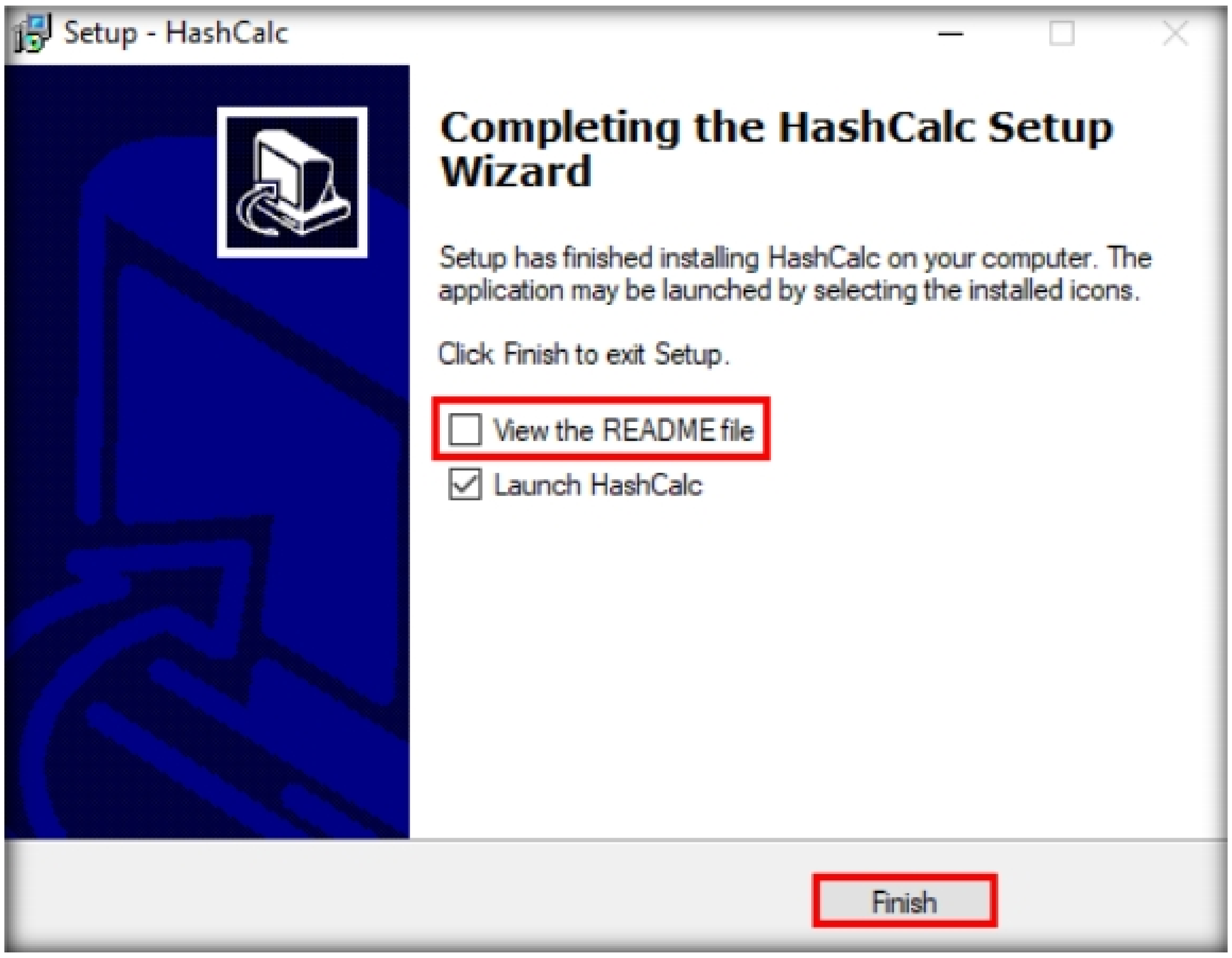
It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Figure 1.1.1: Setup - HashCalc window

4. Follow the installation wizard to install **HashCalc** using all default settings.
5. After the completion of the installation, **Completing the HashCalc Setup Wizard** appears. Uncheck the **View the README file** checkbox and click **Finish**.

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.


Completing the HashCalc Setup Wizard

Setup has finished installing HashCalc on your computer. The application may be launched by selecting the installed icons.

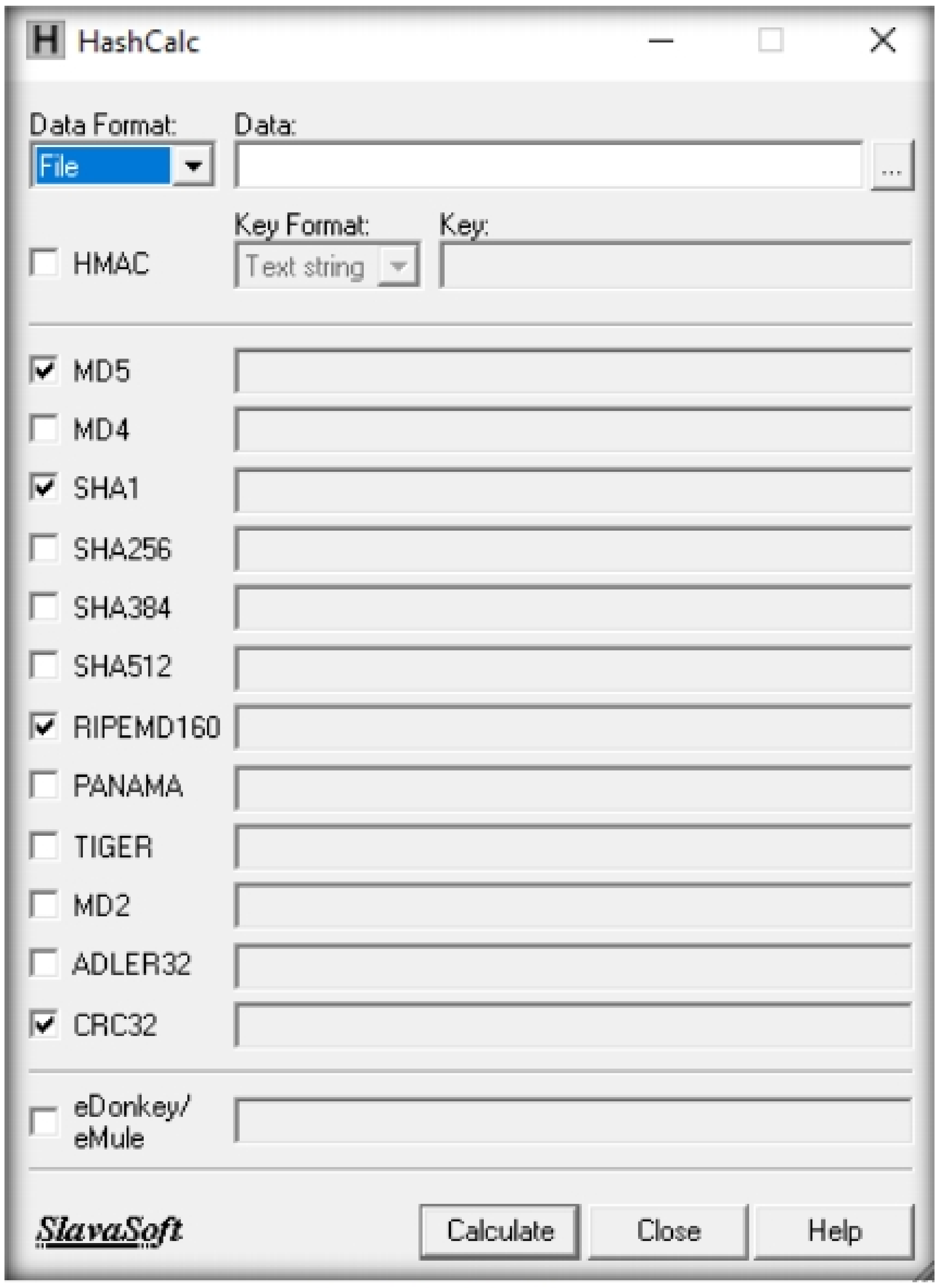
Click Finish to exit Setup.

☐ View the README file

☑ Launch HashCalc

Figure 1.1.2: Setup: Completing HashCalc installation

6. The **HashCalc** main window appears, as shown in the screenshot.


HashCalc
Data:
...
Key Format:
Text string
Key:
SlavaSoft
Calculate
Close
Help

Data Format: File

☐ HMAC

☑ MD5
☐ MD4
☑ SHA1
☐ SHA256
☐ SHA384
☐ SHA512
☑ RIPEMD160
☐ PANAMA
☐ TIGER
☐ MD2
☐ ADLER32
☑ CRC32

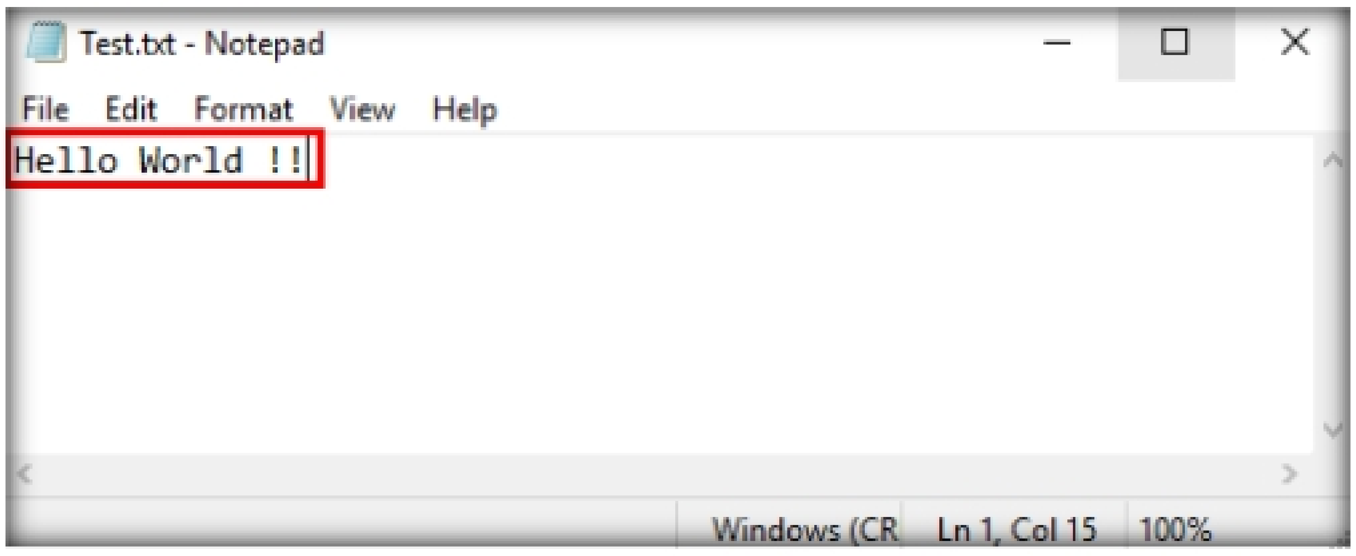
☐ eDonkey/ eMule

Figure 1.1.3: HashCalc Window

7. Minimize the **HashCalc** window. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New** → **Text Document** to create a new text file.

Note: You can create a text file at any location of your choice.

8. A newly created text file appears; rename it to **Test.txt** and open it. Write some text in it (here, **Hello World !!**) and press **Ctrl+S** to save the file. Close the text file.


Test.txt - Notepad
File Edit Format View Help
Windows (CR
Ln 1, Col 15
100%

```
Hello World !!
```

Figure 1.1.4: Test.txt file

TASK 1.2

Calculate Hash Values of a File

9. Now, switch back to the **HashCalc** window; ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon (...) under the **Data** filed.

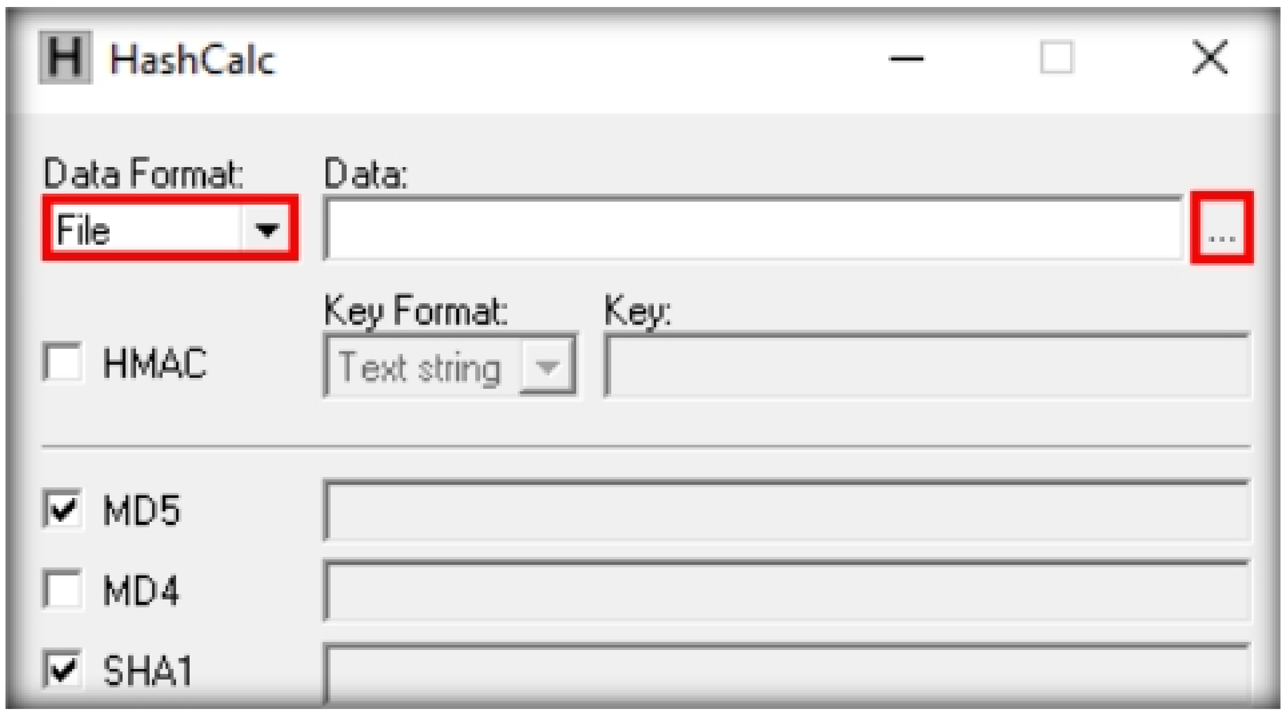

HashCalc
Data Format:
File
Data:
...
HMAC
Key Format:
Text string
Key:
MD5
MD4
SHA1

Figure 1.1.5: Open a text file

10. The **Find** window appears, navigate to the location where you saved the **Test.txt** file (here, **Desktop**) and click **Open**.

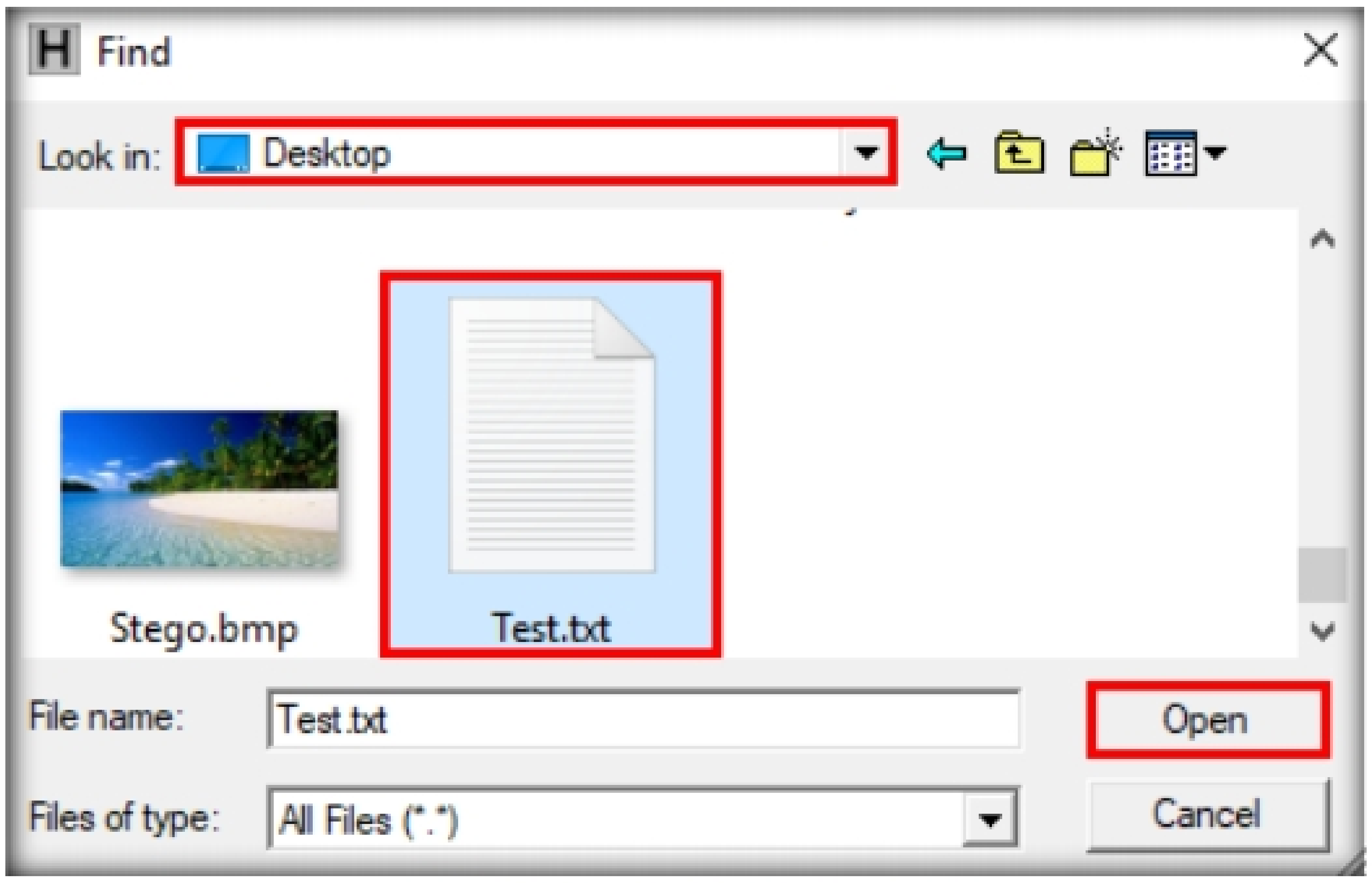
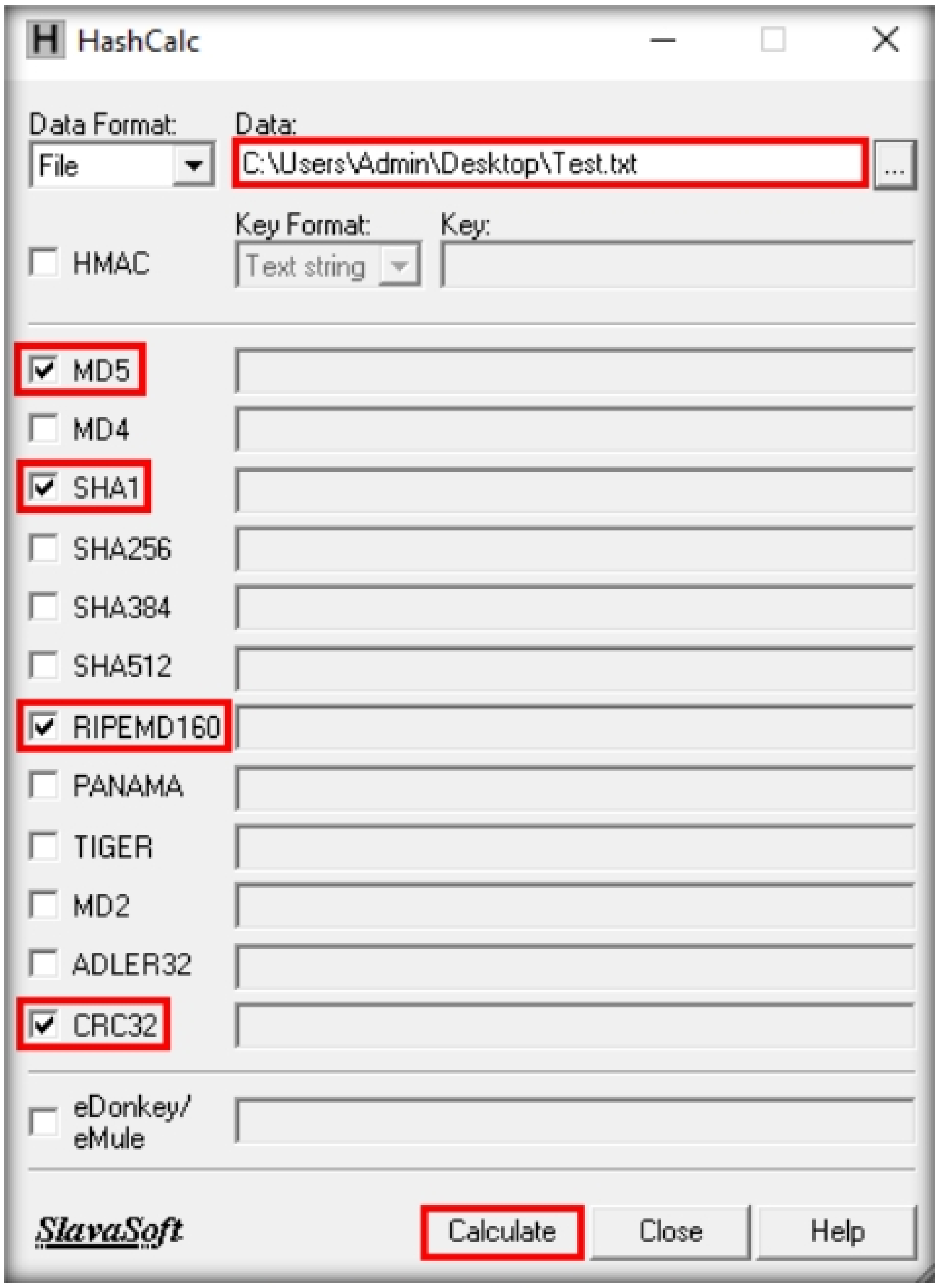

Find
Look in:
Desktop
Stego.bmp
Test.txt
File name:
Test.txt
Files of type:
All Files (*.*)
Open
Cancel

Figure 1.1.6: Find window: select Test.txt file

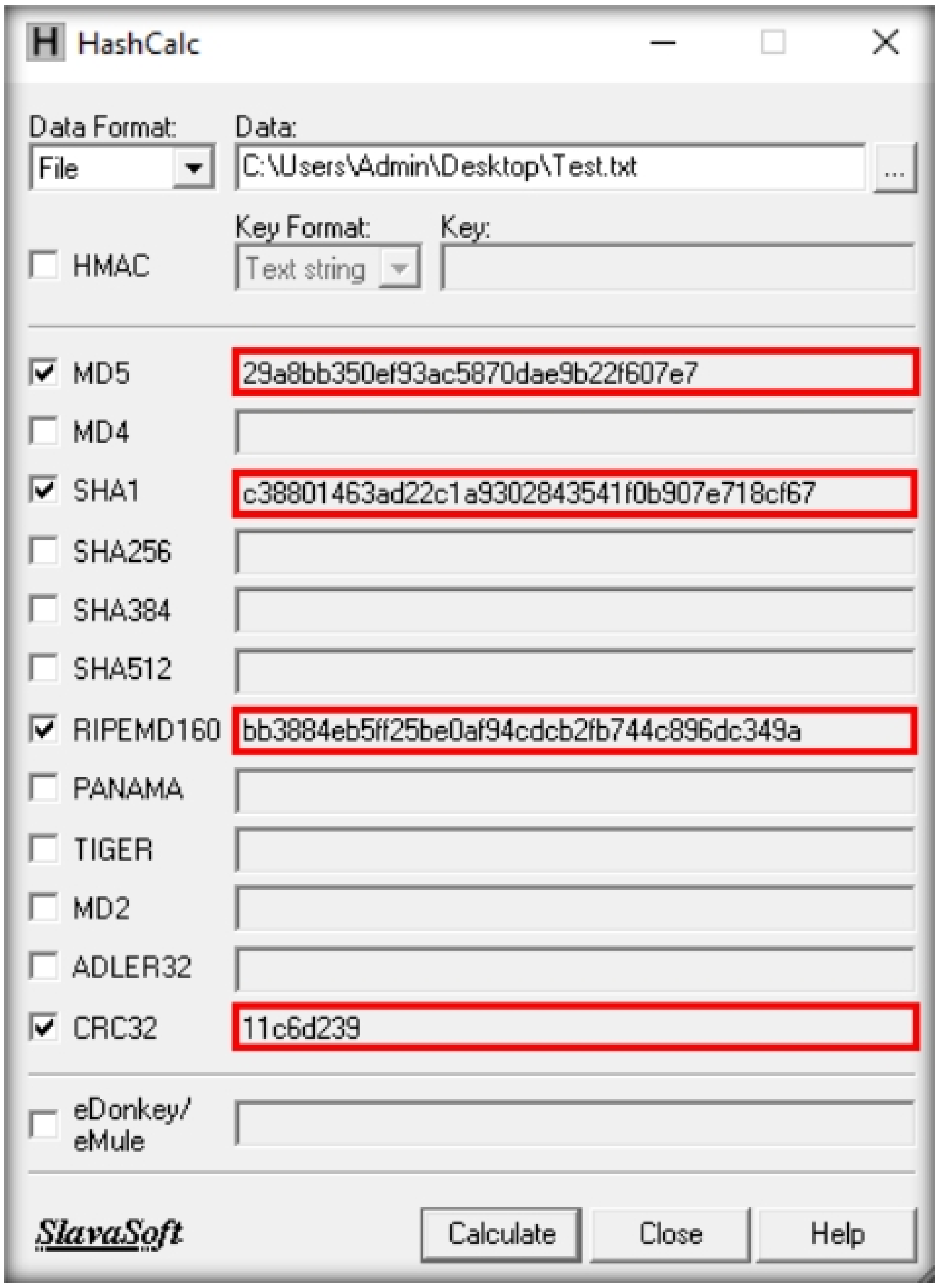
11. The path of the selected file (**Test.txt**) appears under the **Data** field. Ensure that the **MD5**, **SHA1**, **RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.



Data Format: File
Data: C:\Users\Admin\Desktop\Test.txt
☐ HMAC
Key Format: Text string
Key:
☑ MD5
☐ MD4
☑ SHA1
☐ SHA256
☐ SHA384
☐ SHA512
☑ RIPEMD160
☐ PANAMA
☐ TIGER
☐ MD2
☐ ADLER32
☑ CRC32
☐ eDonkey/ eMule

Figure 1.1.7: Calculate hash values of Test.txt file

12. The calculated hash values of the **Test.txt** file appears, as shown in the screenshot.


HashCalc
Calculate
Close
Help
SlavaSoft

Data Format: File

Data: C:\Users\Admin\Desktop\Test.txt

☐ HMAC Key Format: Text string Key:

☑ MD5 29a8bb350ef93ac5870dae9b22f607e7

☐ MD4

☑ SHA1 c38801463ad22c1a9302843541f0b907e718cf67

☐ SHA256

☐ SHA384

☐ SHA512

☑ RIPEMD160 bb3884eb5ff25be0af94cdcb2fb744c896dc349a

☐ PANAMA

☐ TIGER

☐ MD2

☐ ADLER32

☑ CRC32 11c6d239

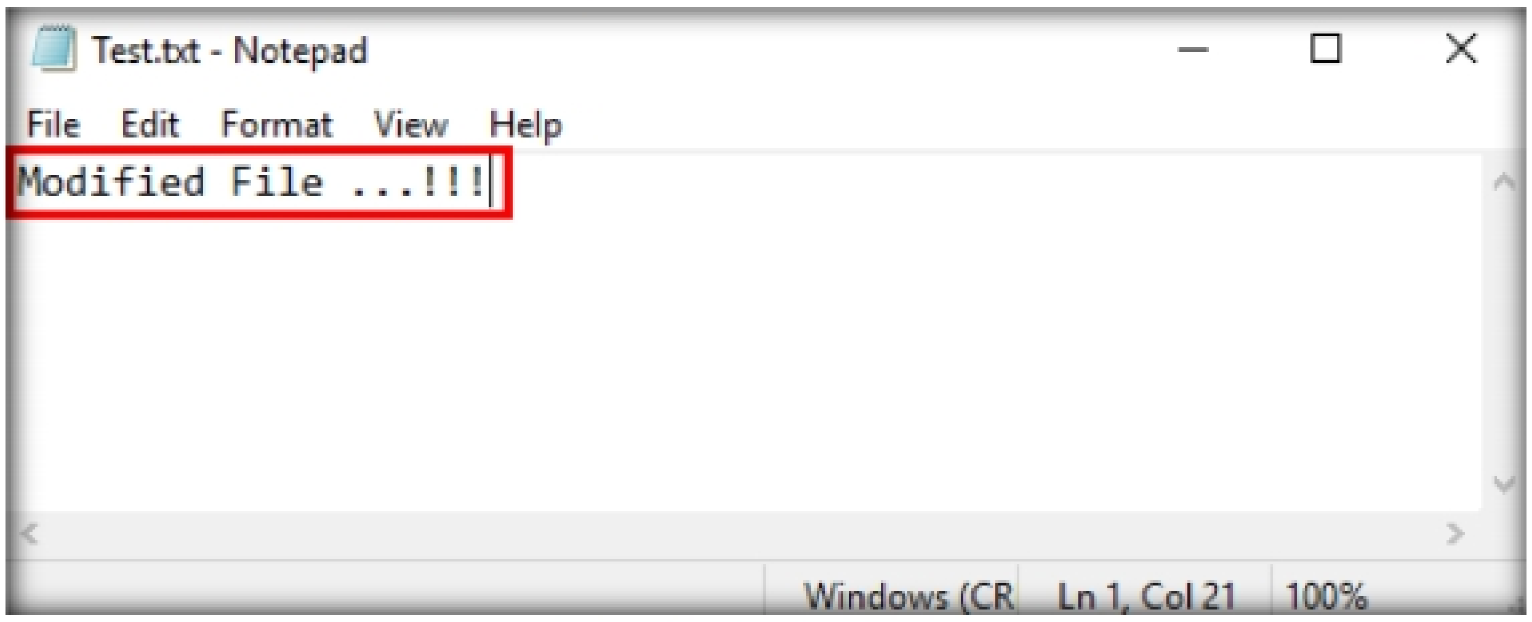
☐ eDonkey/ eMule

Figure 1.1.8: Calculated hash values of Test.txt file

TASK 1.3

Modify File Content

13. Minimize the **HashCalc** window, navigate to **Desktop**, and double-click the **Test.txt** file to open it. Modify the file content by writing some text (here, **Modified File ...!!!**) and press **Ctrl+S** to save it. Close the text file.


Test.txt - Notepad
File
Edit
Format
View
Help
Windows (CR
Ln 1, Col 21
100%

```
Modified File ...!!!
```

Figure 1.1.9: Modify text content

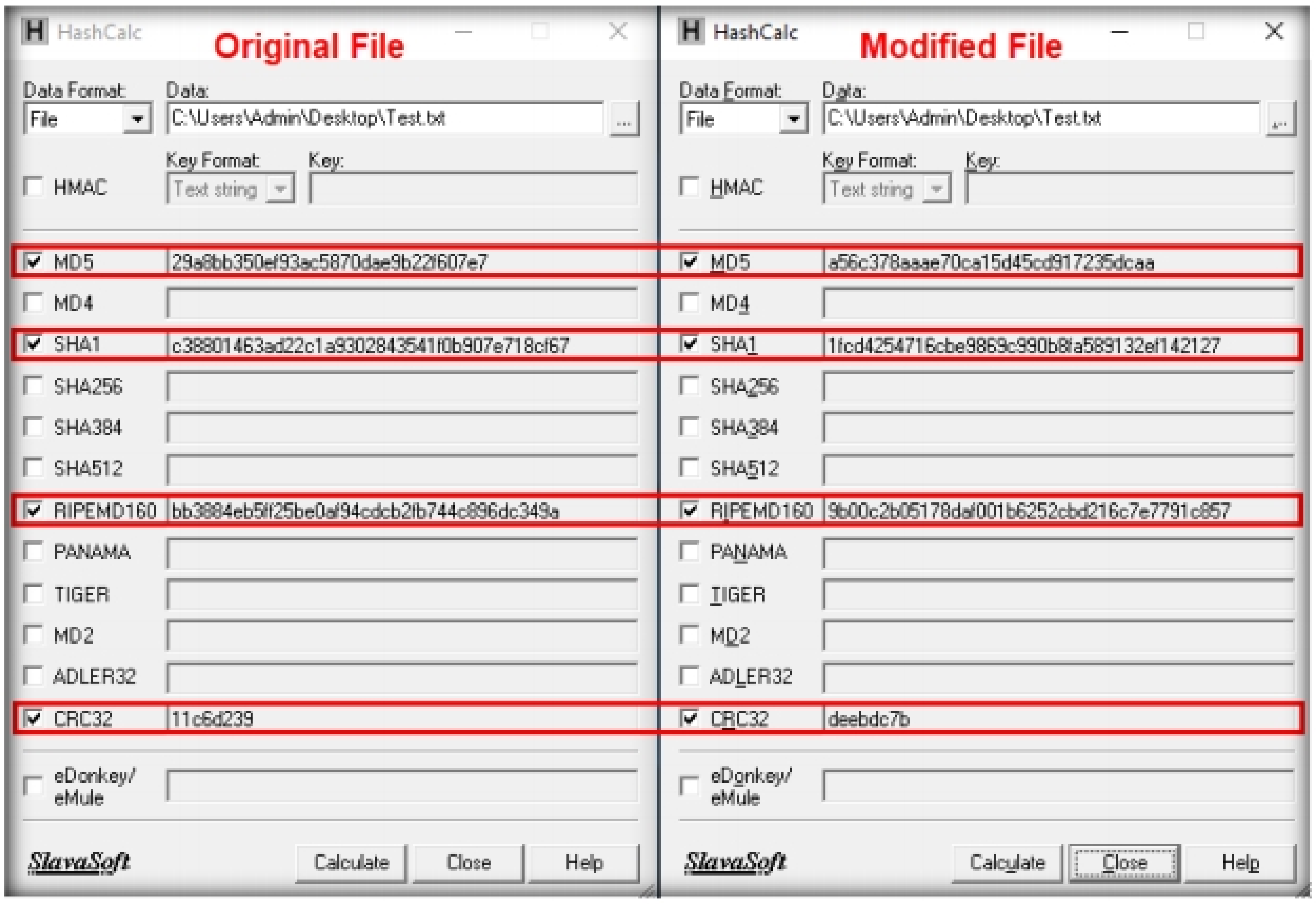
14. Now, double-click **HashCalc** shortcut from **Desktop** to launch another HashCalc window.

15. A new **HashCalc** window appears, perform **Steps #9-12**.

TASK 1.4

Compare Hash Values of Original and Modified File

16. Now, maximize the first **HashCalc** window and place it beside the second **HashCalc** window. You can observe changes in the hash values of the text file (**Test.txt**) before and after the modification, as shown in the screenshot.



	Original File	Modified File
Data Format	File	File
Data	C:\Users\Admin\Desktop\Test.txt	C:\Users\Admin\Desktop\Test.txt
☑ MD5	29a8bb350ef93ac5870dae9b22f607e7	a56c378aaae70ca15d45cd917235dcaa
☑ SHA1	c38801463ad22c1a9302843541f0b907e718cf67	1fcd4254716cbe9869c990b8fa589132ef142127
☑ RIPEMD160	bb3884eb5ff25be0af94cdcb2fb744c896dc349a	9b00c2b05178daf001b6252cbd216c7e7791c857
☑ CRC32	11c6d239	deebdc7b

Figure 1.1.10: Difference in Hash values of the same text file

Note: In real-time, the HashCalc tool is used to check the integrity of a file where the changes in the hash values indicate that the file content has been modified.

17. This concludes the demonstration of calculating one-way hashes using HashCalc.

18. Close all open windows and document all the acquired information.

TASK 2

Calculate MD5 Hashes using MD5 Calculator

Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

TASK 2.1

Install MD5 Calculator Tool

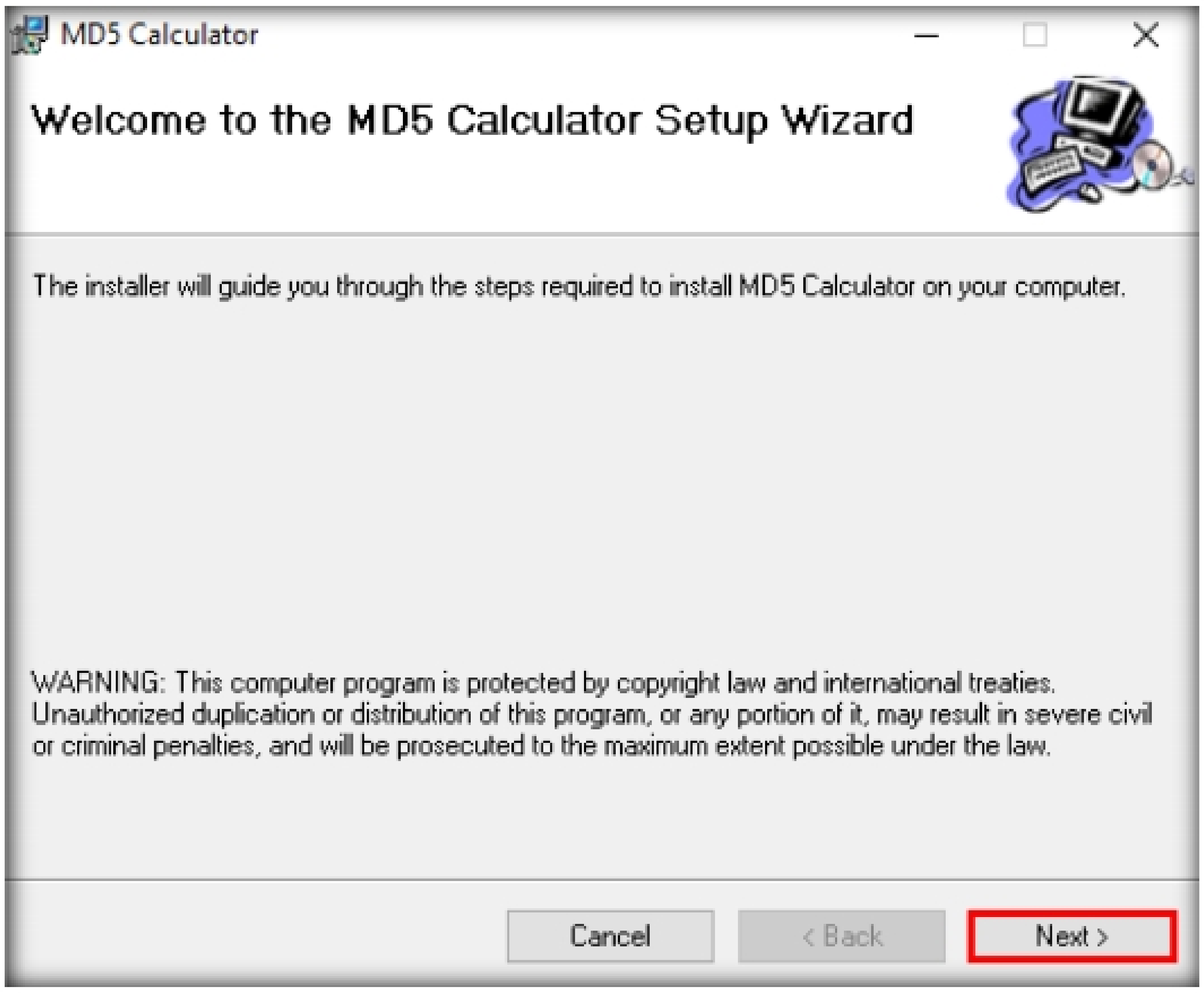
1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator** and double-click **md5calc(1.0.0.0).msi**.

2. The **MD5 Calculator** setup window appears; click **Next**.

MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.



Welcome to the MD5 Calculator Setup Wizard

The installer will guide you through the steps required to install MD5 Calculator on your computer.

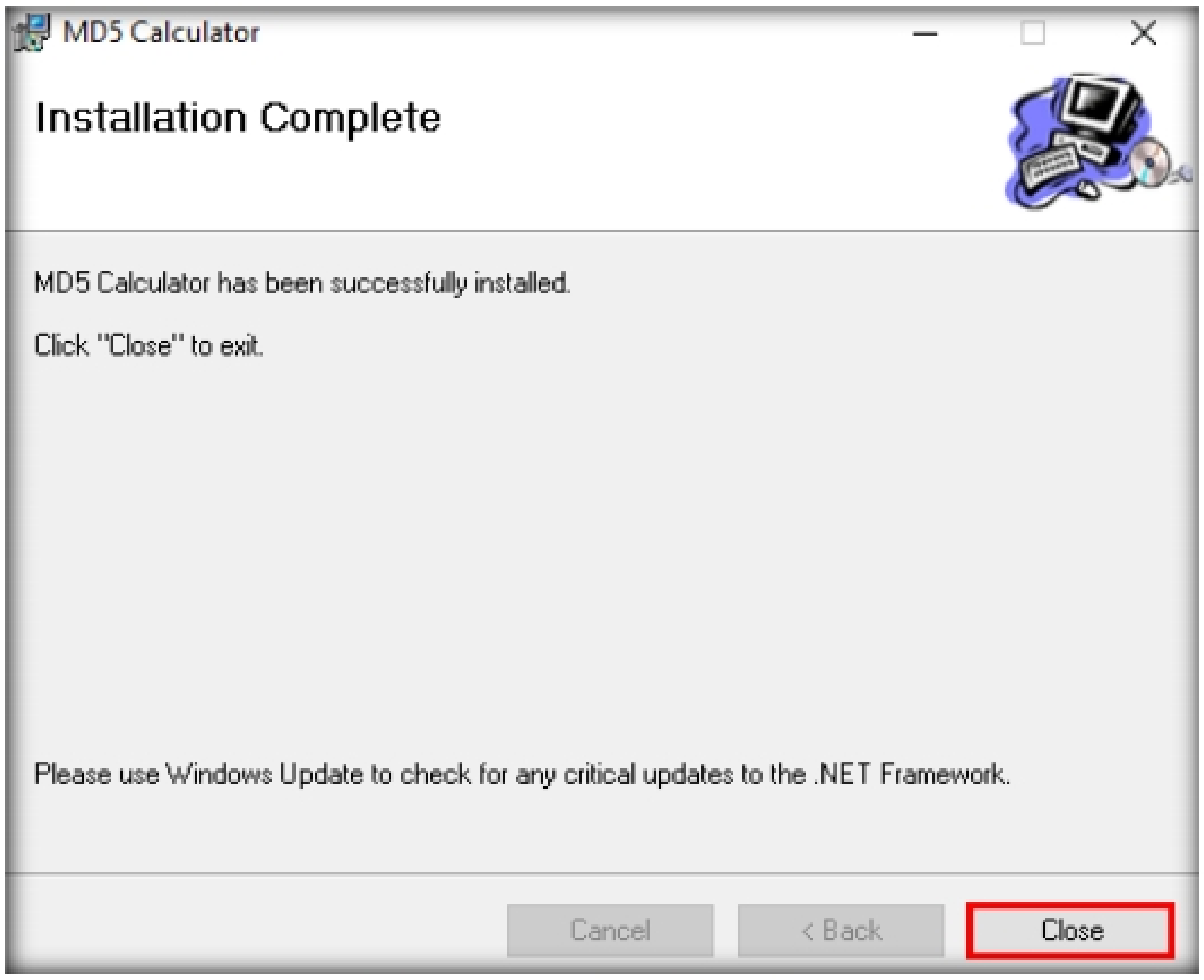
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Figure 1.2.1: MD5 Calculator Window

3. Follow the installation wizard to install the **MD5 Calculator** using all default settings.

Note: If a **User Account Control** pop-up appears, click **Yes**.

4. After the completion of the installation, the **Installation Complete** wizard appears; click **Close**.



Installation Complete

MD5 Calculator has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Figure 1.2.2: Installation Complete wizard

TASK 2.2

Calculate MD5 Value of an Original File

5. Navigate to **Desktop**, right-click on the text file (**Test.txt**) that we created in the previous task, and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

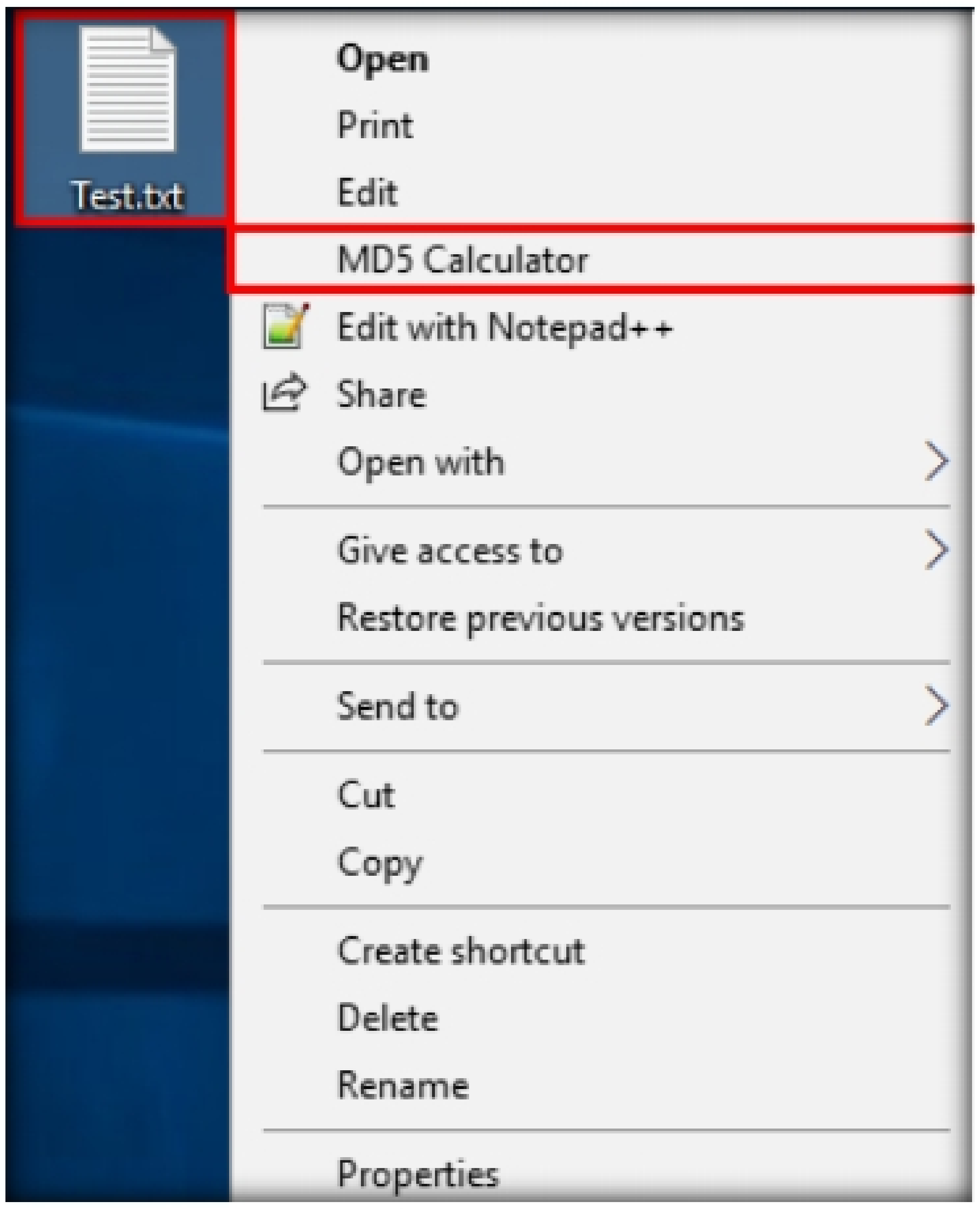
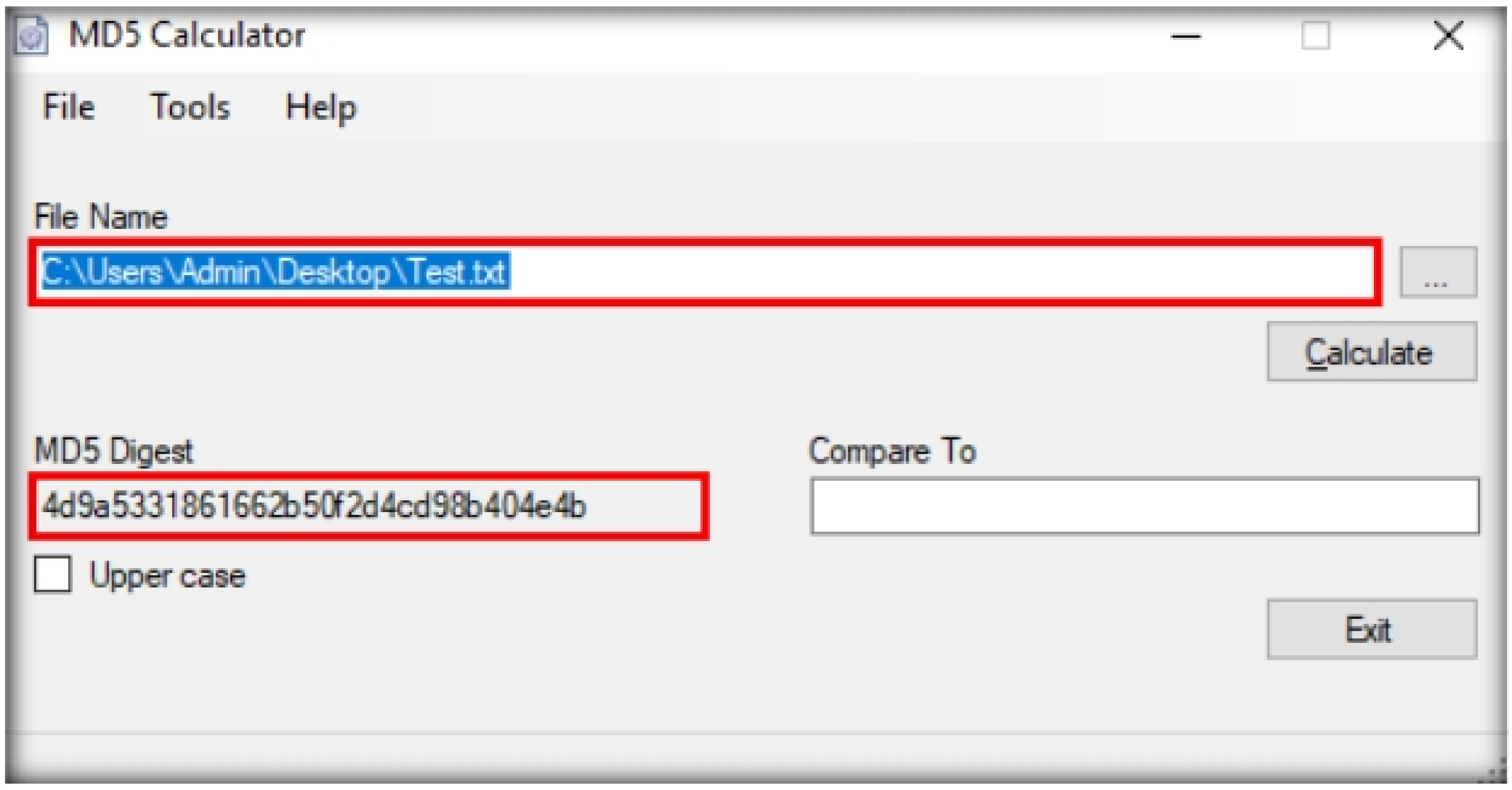

Test.txt
Open
Print
Edit
MD5 Calculator
Edit with Notepad++
Share
Open with
Give access to
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

Figure 1.2.3: Calculate MD5 hash of Test.txt file

6. The **MD5 Calculator** window appears, with the path of file under the **File Name** field and MD5 hash value under the **MD5 Digest** field, as shown in the screenshot.

7. Copy the MD5 hash value from the **MD5 Digest** field.


MD5 Calculator
File
Tools
Help
...
Calculate
Exit

File Name: C:\Users\Admin\Desktop\Test.txt

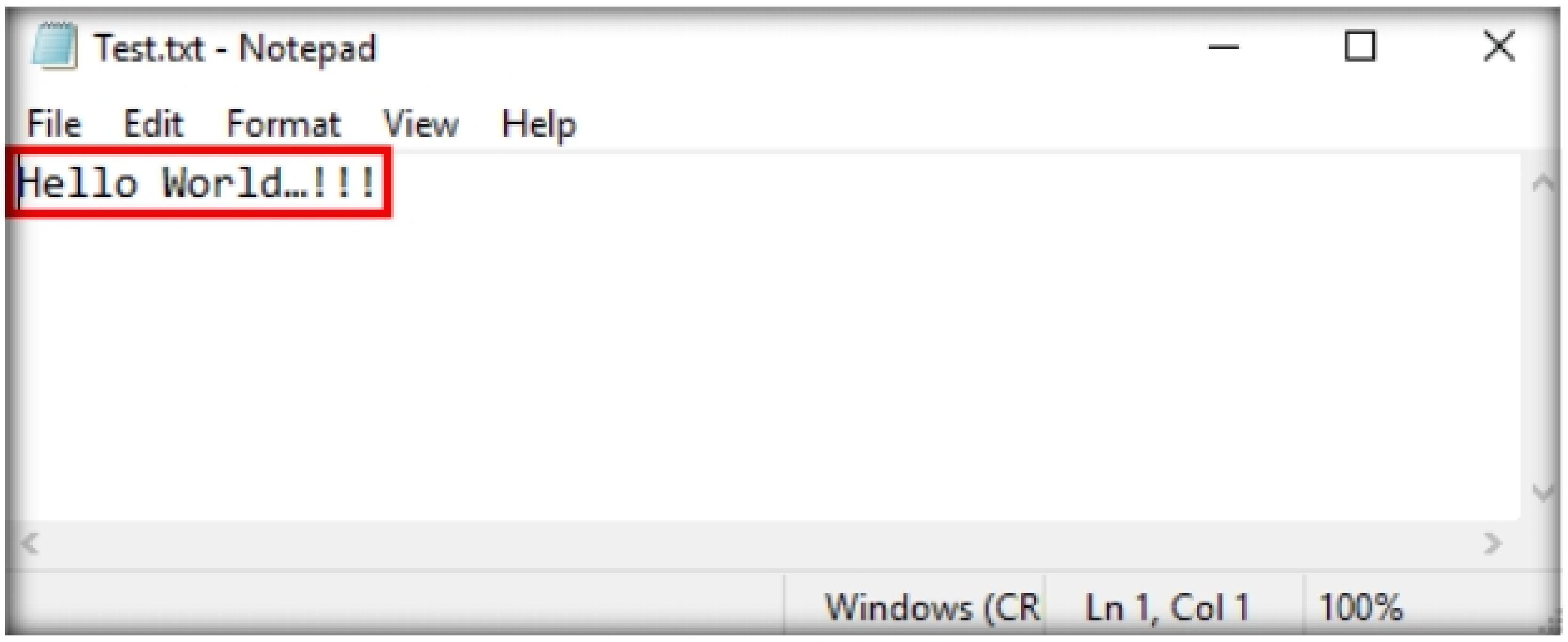
MD5 Digest: 4d9a5331861662b50f2d4cd98b404e4b

Compare To:

☐ Upper case

Figure 1.2.4: MD5 Calculator window with the MD5 hash value of the file

8. Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by inserting text within (here, **Hello World…!!!**). Save and close the **Test.txt** file.



```
Hello World…!!!
```

Figure 1.2.5: Modify the file content

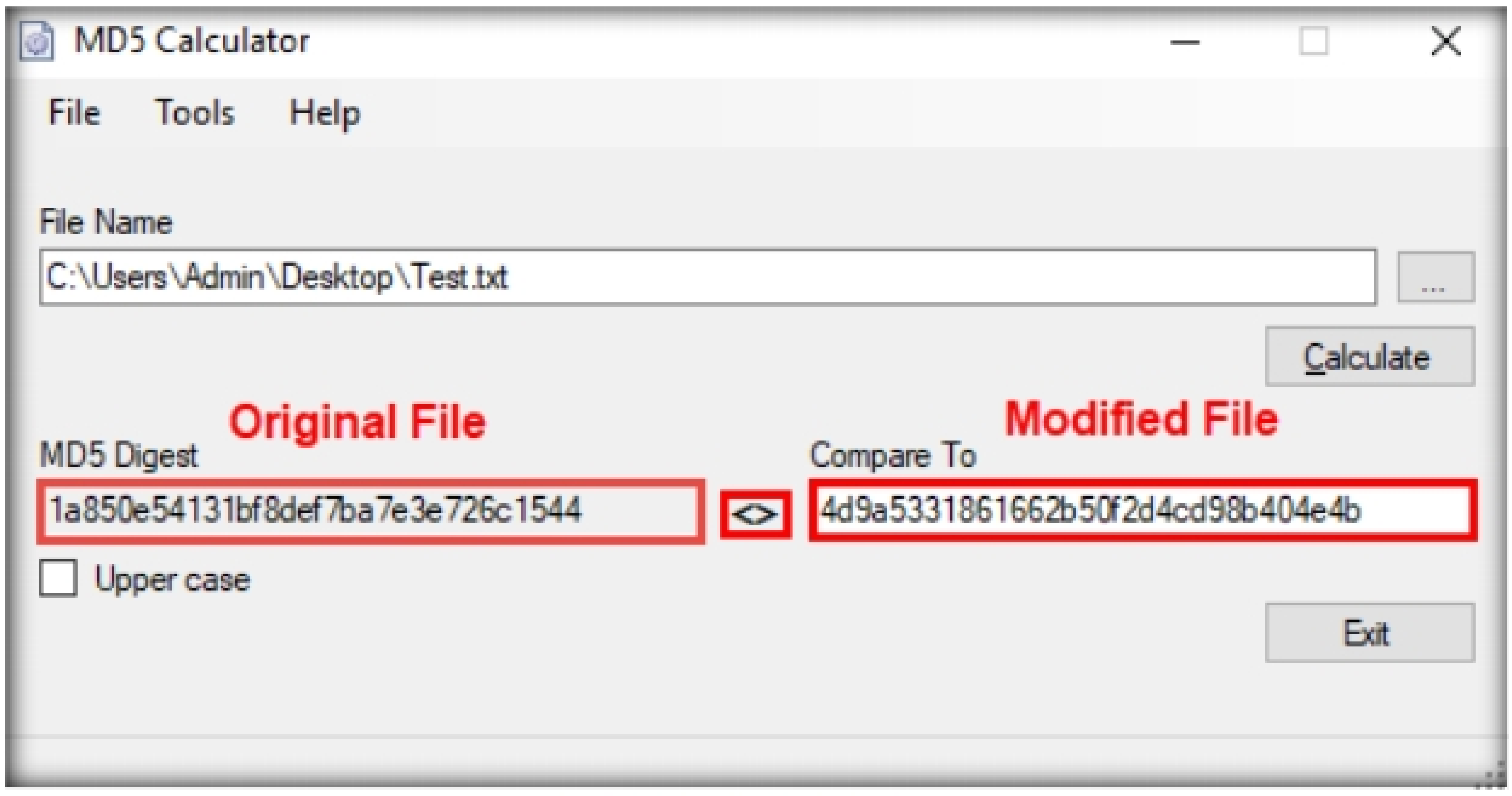
9. After changing the file content, again right-click on the text file (**Test.txt**) and click **MD5 Calculator** from the context menu to calculate the MD5 hash of the file.

TASK 2.3

Analyze MD5 Values of Original and Modified File

10. A new **MD5 Calculator** window appears, with the MD5 hash value under the **MD5 Digest** field. In the **Compare To** field, paste the copied MD5 hash value of the file before it was modified.

11. The symbol (**<>**) between the **MD5 Digest** and **Compare To** fields indicates that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.



File Name: C:\Users\Admin\Desktop\Test.txt

MD5 Digest: 1a850e54131bf8def7ba7e3e726c1544

Compare To: 4d9a5331861662b50f2d4cd98b404e4b

☐ Upper case

Figure 1.2.6: Modify the file content

Note: If a person wants to send a file to another person via a medium, they will calculate its hashes and send the file (along with the hash value) to the intended person. When the intended person receives the email, they will download the file and calculate its value using the MD5 Calculator.

The recipient compares the generated hash value with the hash value that was sent through email: if both tally, it is evident that they received the file without any modifications by a third person and that the integrity of the file is intact.

12. This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.
13. Close all open windows and document all the acquired information.

TASK 3

Calculate MD5 Hashes using HashMyFiles

Here, we will use the HashMyFiles tool to calculate MD5 hashes.

TASK 3.1

Install HashMyFiles Tool

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double-click **HashMyFiles.exe**.
2. The **HashMyFiles** main window appears, as shown in the screenshot.

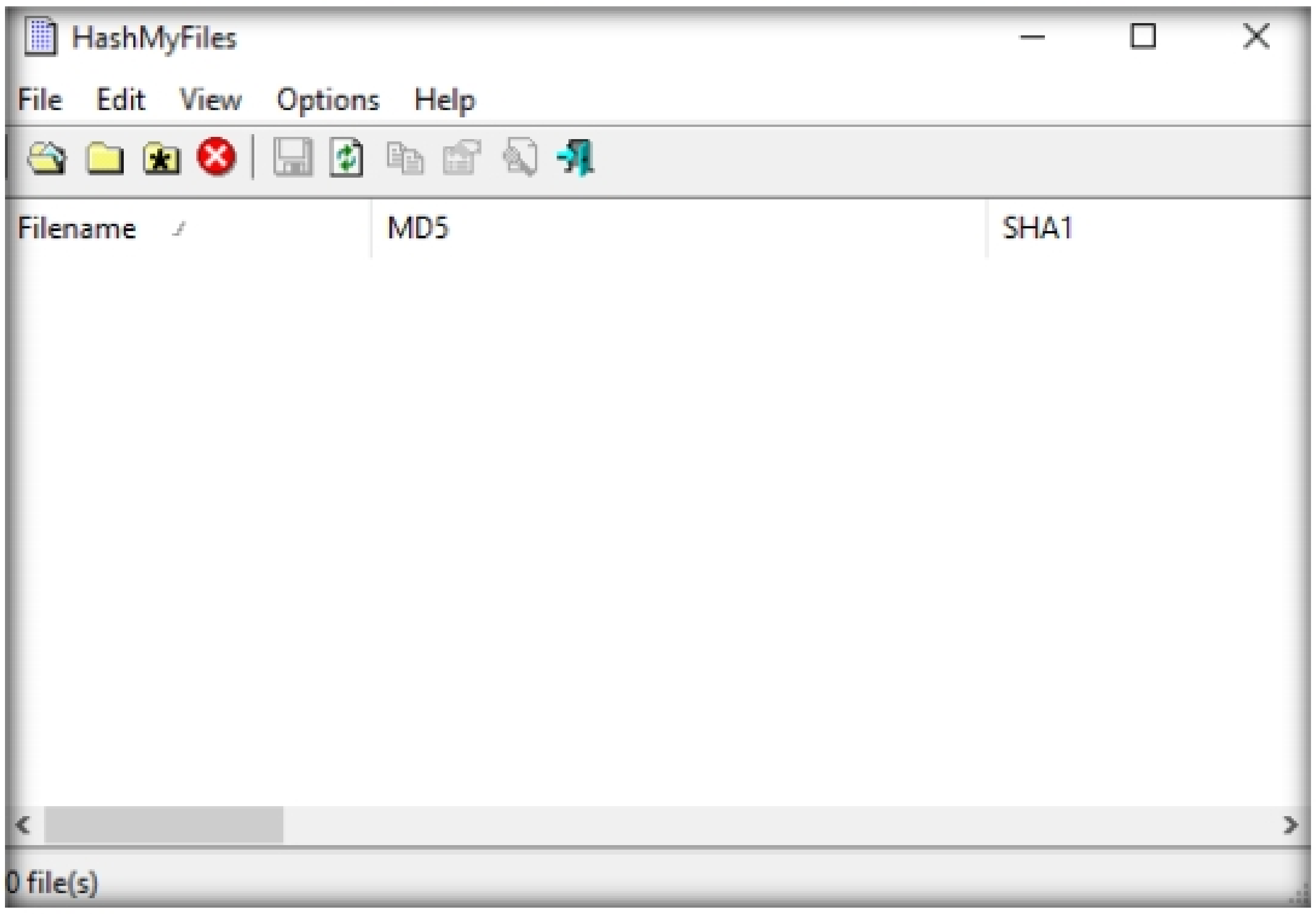

HashMyFiles
File Edit View Options Help
Filename
MD5
SHA1
0 file(s)

Figure 1.3.1 HashMyFiles window

3. In the **HashMyFiles** window, click **Files** from the menu bar. From the drop-down list, click the **Add Folder** option.

Note: You can also use the **Add Files** option to add multiple files.

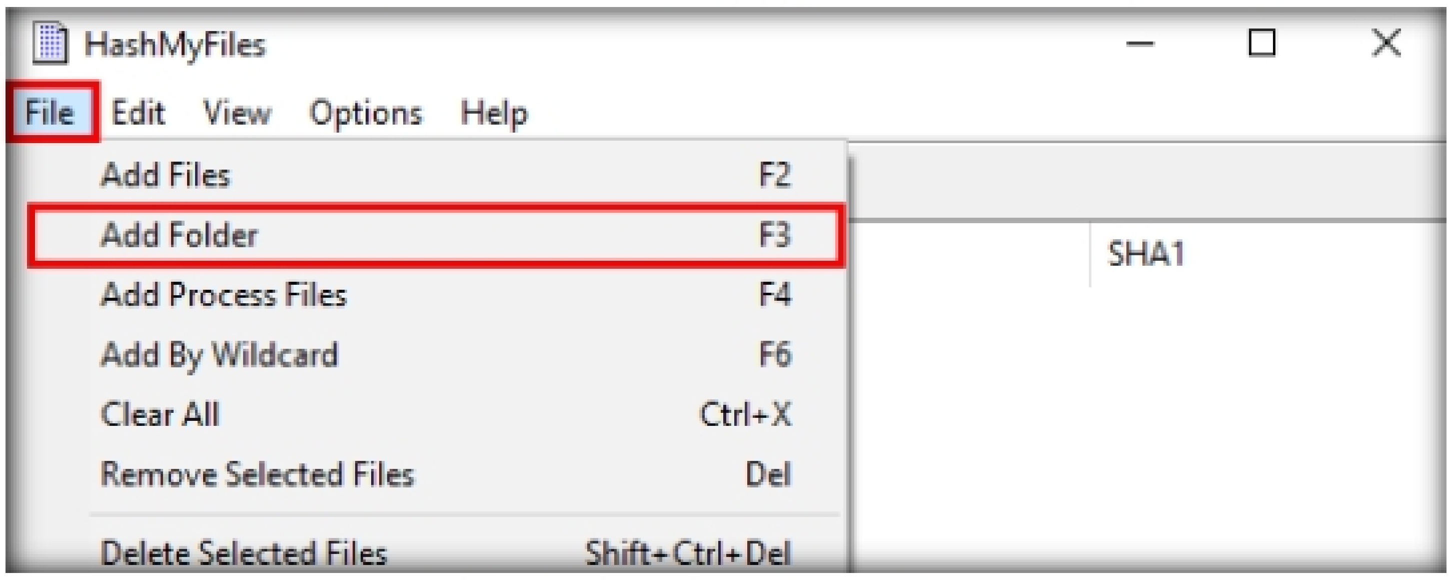

HashMyFiles
File Edit View Options Help
Add Files F2
Add Folder F3
Add Process Files F4
Add By Wildcard F6
Clear All Ctrl+X
Remove Selected Files Del
Delete Selected Files Shift+Ctrl+Del
SHA1

Figure 1.3.2: HashMyFiles window: File options

4. The **Select Folder** pop-up appears; click on the ellipsis icon (...) to select the folder you want to encrypt.

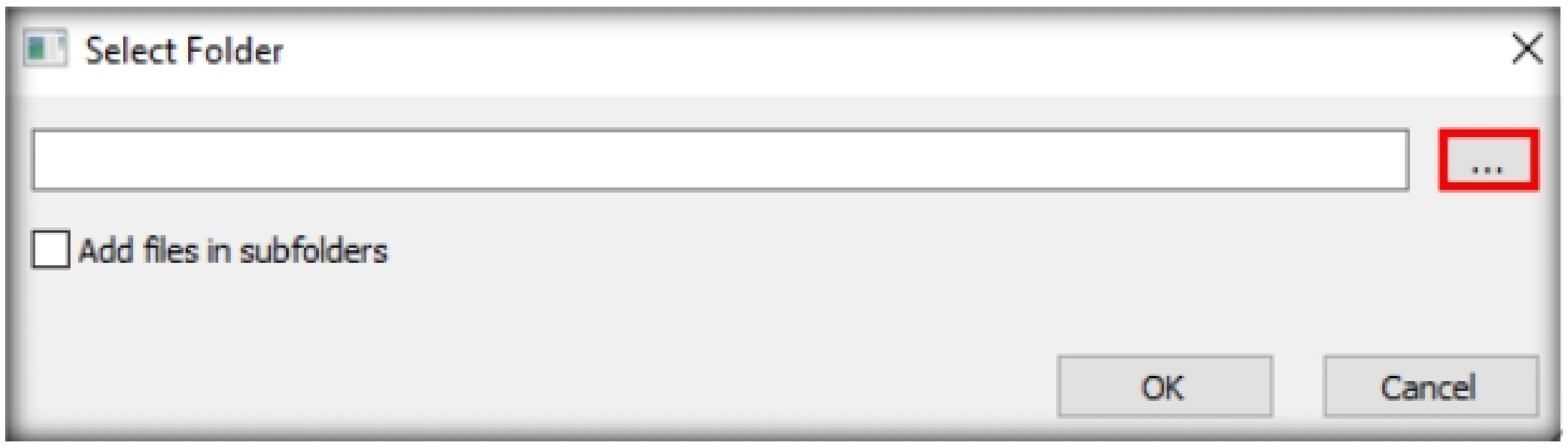
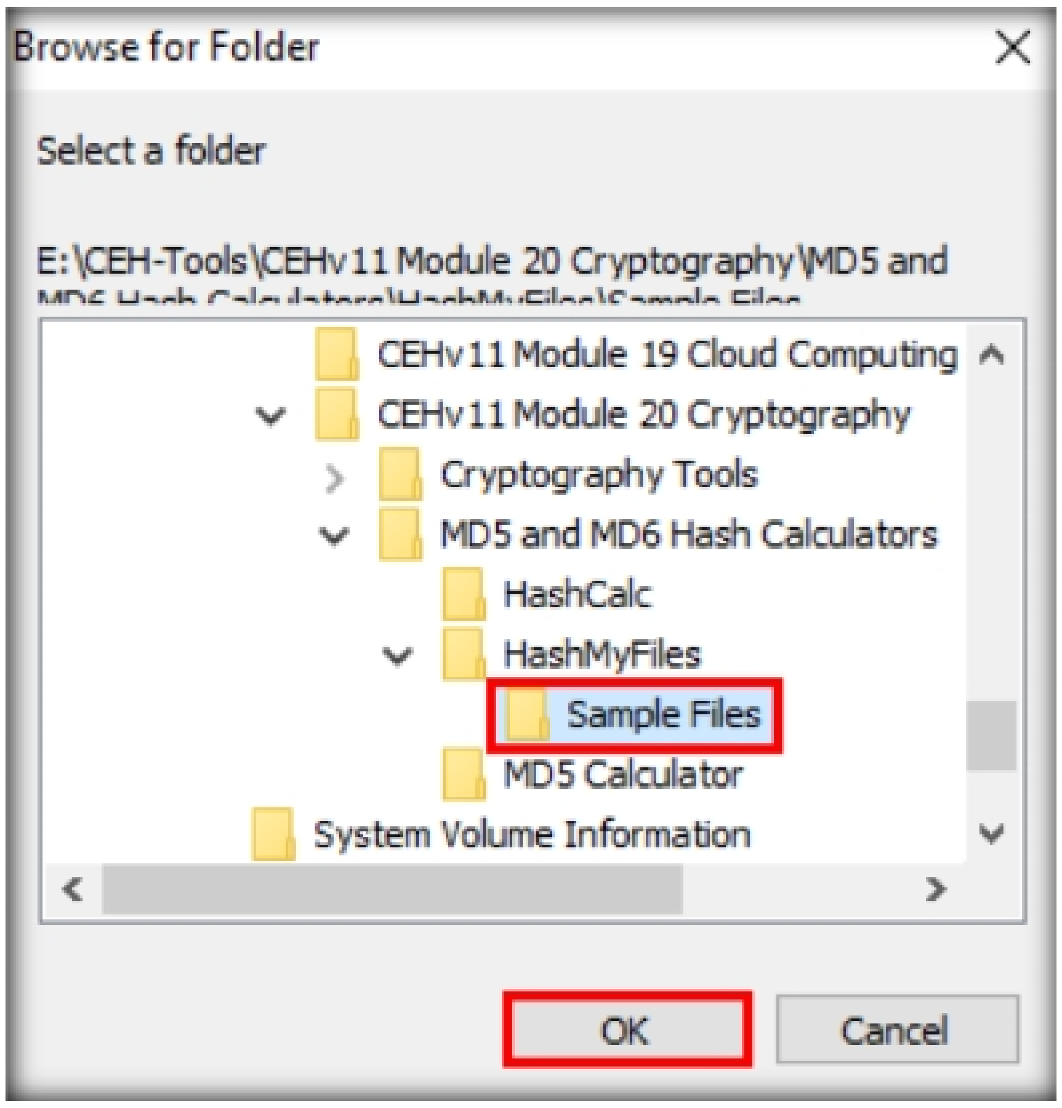

Select Folder
...
☐ Add files in subfolders
OK
Cancel

Figure 1.3.3: Select Folder pop-up

5. The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

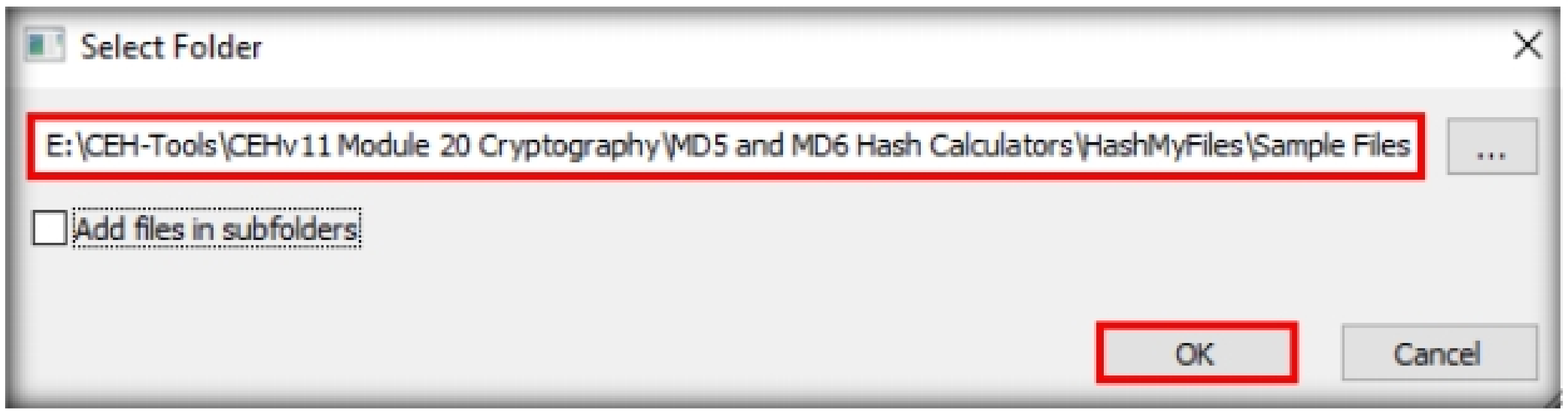
Note: You can select any folder of your choice that you wish to encrypt.


Browse for Folder
Select a folder
CEHv11 Module 19 Cloud Computing
CEHv11 Module 20 Cryptography
Cryptography Tools
MD5 and MD6 Hash Calculators
HashCalc
HashMyFiles
Sample Files
MD5 Calculator
System Volume Information
OK
Cancel

E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and

Figure 1.3.4: Browse for Folder

6. The location of the selected folder appears in the field; click **OK**.


Select Folder
...
☐ Add files in subfolders
OK
Cancel

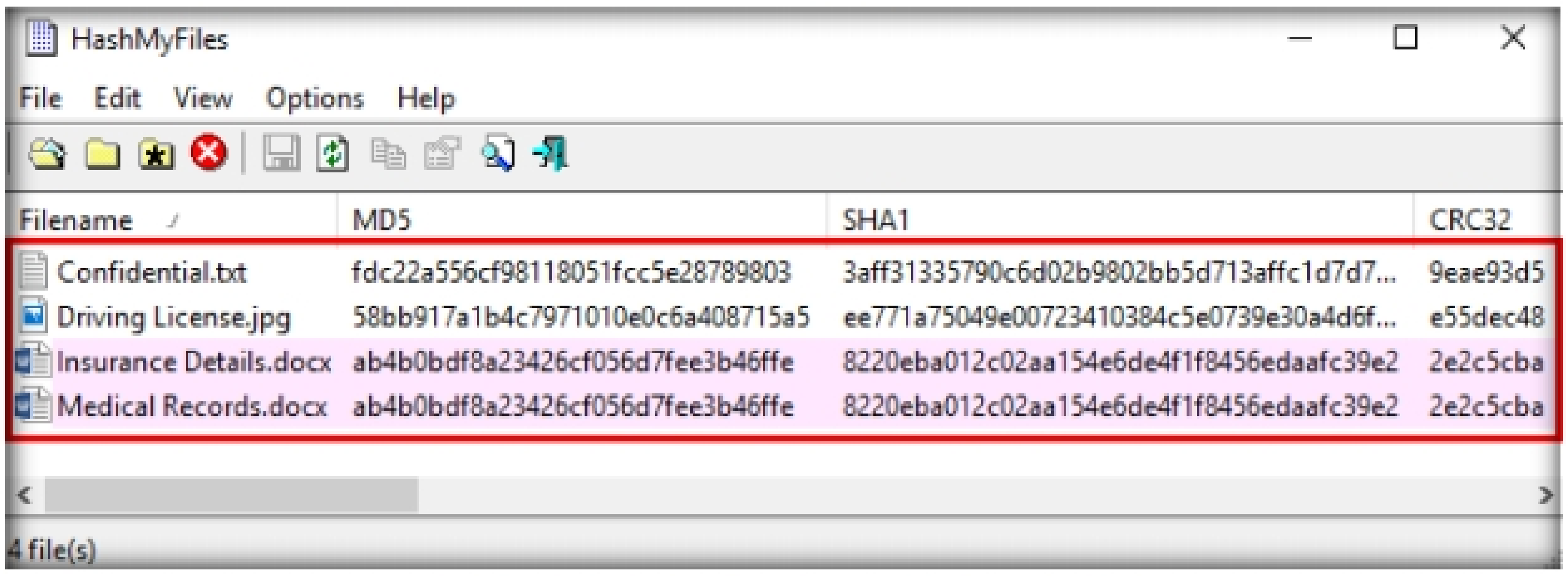
E:\CEH-Tools\CEHv11 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles\Sample Files

Figure 1.3.5: Select Folder pop-up: Selected folder's location

TASK 3.2

Analyze MD5 Values

7. A list of files contained in the folder appears, along with their various hash values such as **MD5**, **SHA1**, **CRC32**, etc.


HashMyFiles
File Edit View Options Help
4 file(s)

Filename	MD5	SHA1	CRC32
Confidential.txt	fdc22a556cf98118051fcc5e28789803	3aff31335790c6d02b9802bb5d713affc1d7d7...	9eae93d5
Driving License.jpg	58bb917a1b4c7971010e0c6a408715a5	ee771a75049e00723410384c5e0739e30a4d6f...	e55dec48
Insurance Details.docx	ab4b0bdf8a23426cf056d7fee3b46ffe	8220eba012c02aa154e6de4f1f8456edaafc39e2	2e2c5cba
Medical Records.docx	ab4b0bdf8a23426cf056d7fee3b46ffe	8220eba012c02aa154e6de4f1f8456edaafc39e2	2e2c5cba

Figure 1.3.6: HashMyFiles window: list of files with hash values

You can also use other MD5 and MD6 hash calculators such as **MD6 Hash Generator** (https://www.browserling.com), **All Hash Generator** (https://www.browserling.com), **MD6 Hash Generator** (https://convert-tool.com), and **md5 hash calculator** (https://onlinehashtools.com) to calculate MD5 and MD6 hashes.

8. In the **HashMyFiles** window, click **Options** from the menu bar and choose **Hash Types** from the options. You can observe a list of hash functions such as **MD5**, **SHA1**, **CRC32**, **SHA-256**, **SHA-512**, and **SHA-384**, which you can choose (here, the MD5, SHA1, and CRC32 hash functions were selected).

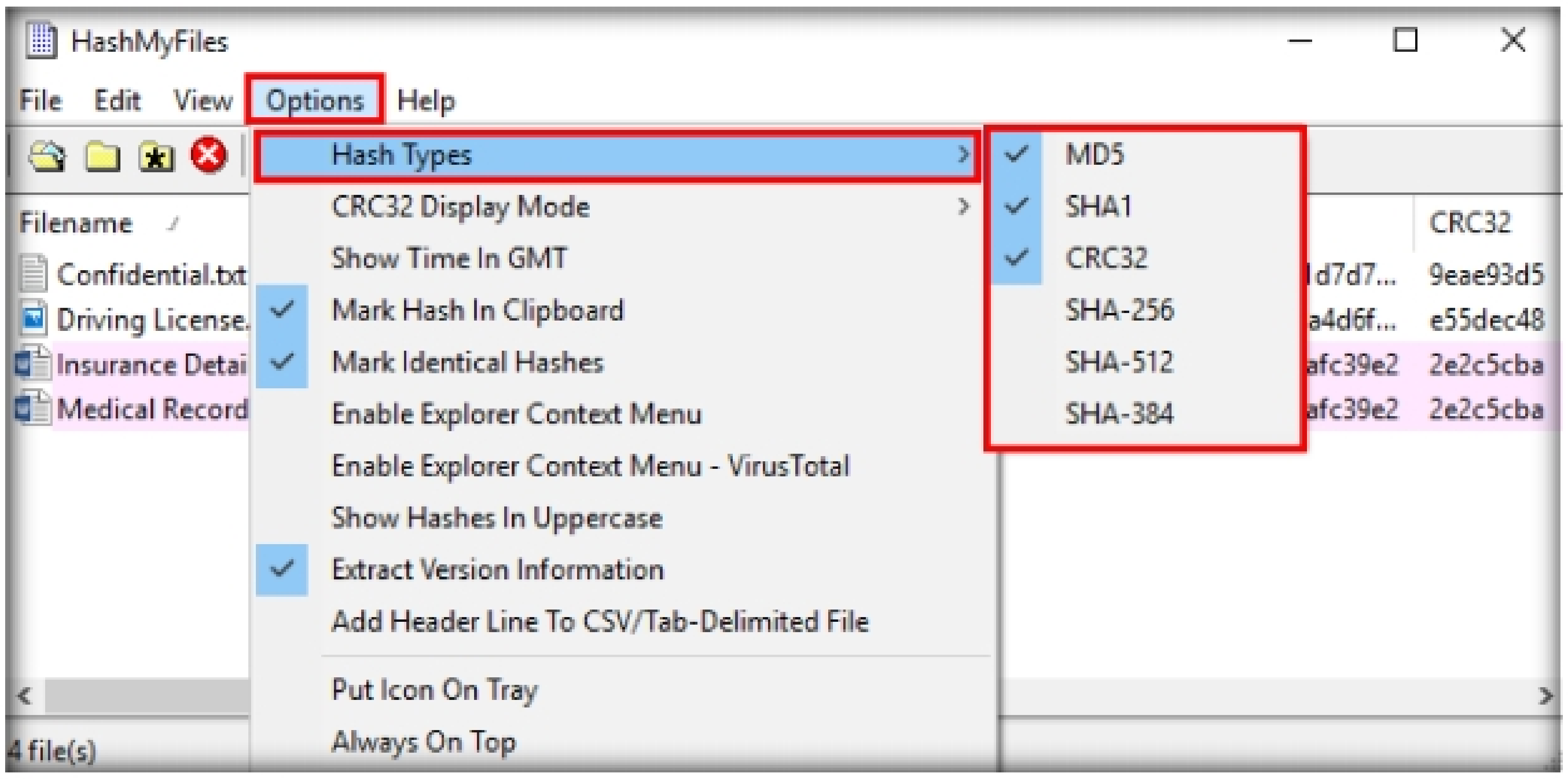

HashMyFiles
File Edit View Options Help
Hash Types
CRC32 Display Mode
Show Time In GMT
✓ Mark Hash In Clipboard
✓ Mark Identical Hashes
Enable Explorer Context Menu
Enable Explorer Context Menu - VirusTotal
Show Hashes In Uppercase
✓ Extract Version Information
Add Header Line To CSV/Tab-Delimited File
Put Icon On Tray
Always On Top
✓ MD5
✓ SHA1
✓ CRC32
SHA-256
SHA-512
SHA-384
Filename
CRC32
Confidential.txt
Driving License.
Insurance Detai
Medical Record
4 file(s)

Figure 1.3.7: HashMyFiles window: Options list

Note: In real-time, you may share confidential information in the folder in an encrypted form to maintain its integrity.

9. This concludes the demonstration of calculating MD5 hashes using HashMyFiles.

10. Close all open windows and document all the acquired information.

TASK 4

Perform File and Text Message Encryption using CryptoForge

Here, we will use the CryptoForge tool to encrypt a file and text message.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine; log in with the credentials **Administrator**/**Pa$$w0rd**.

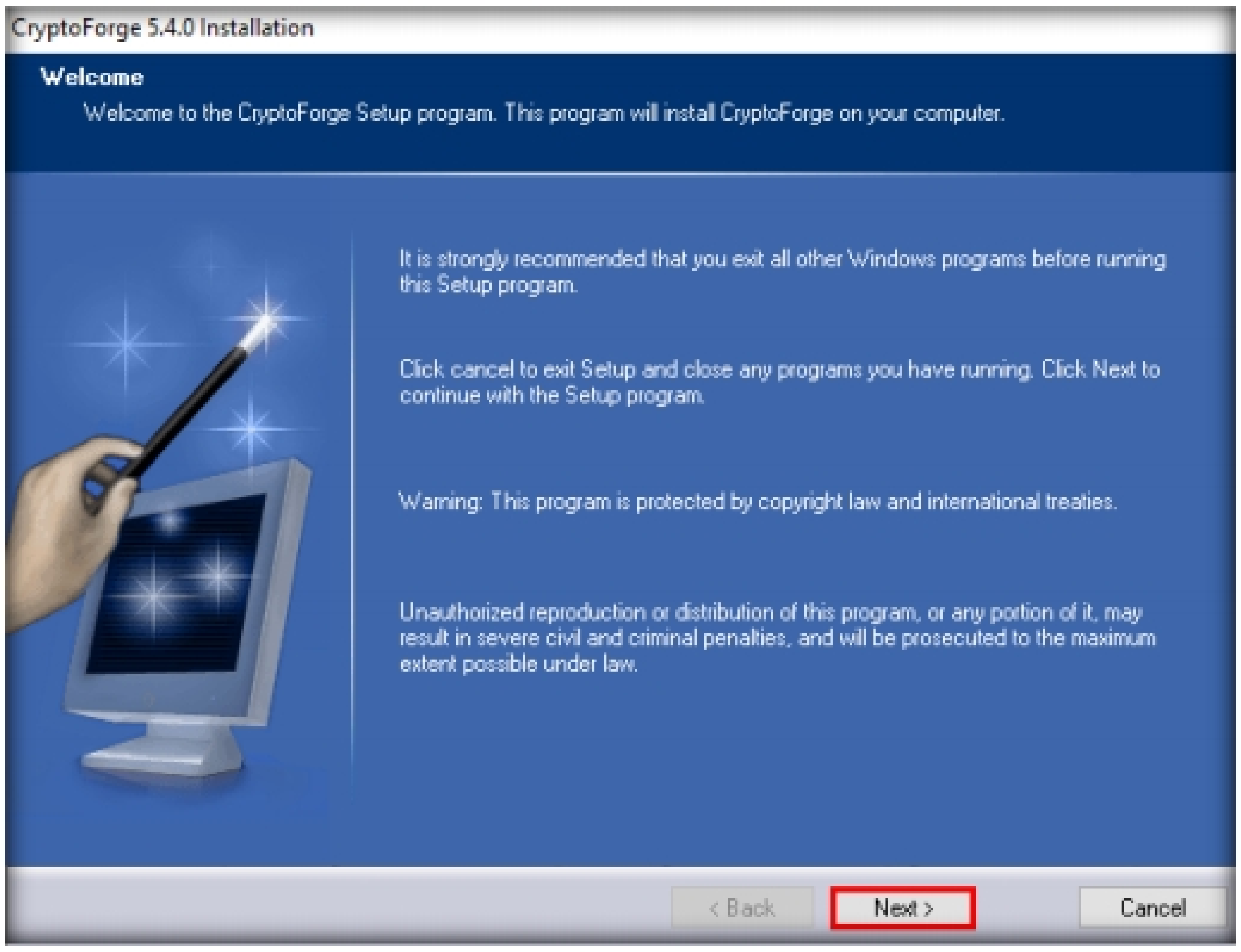
TASK 4.1

Install CryptoForge

2. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge** and double-click **CryptoForge.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

3. The **CryptoForge Installation** window appears; click **Next**.



Welcome

Welcome to the CryptoForge Setup program. This program will install CryptoForge on your computer.

It is strongly recommended that you exit all other Windows programs before running this Setup program.

Click cancel to exit Setup and close any programs you have running. Click Next to continue with the Setup program.

Warning: This program is protected by copyright law and international treaties.

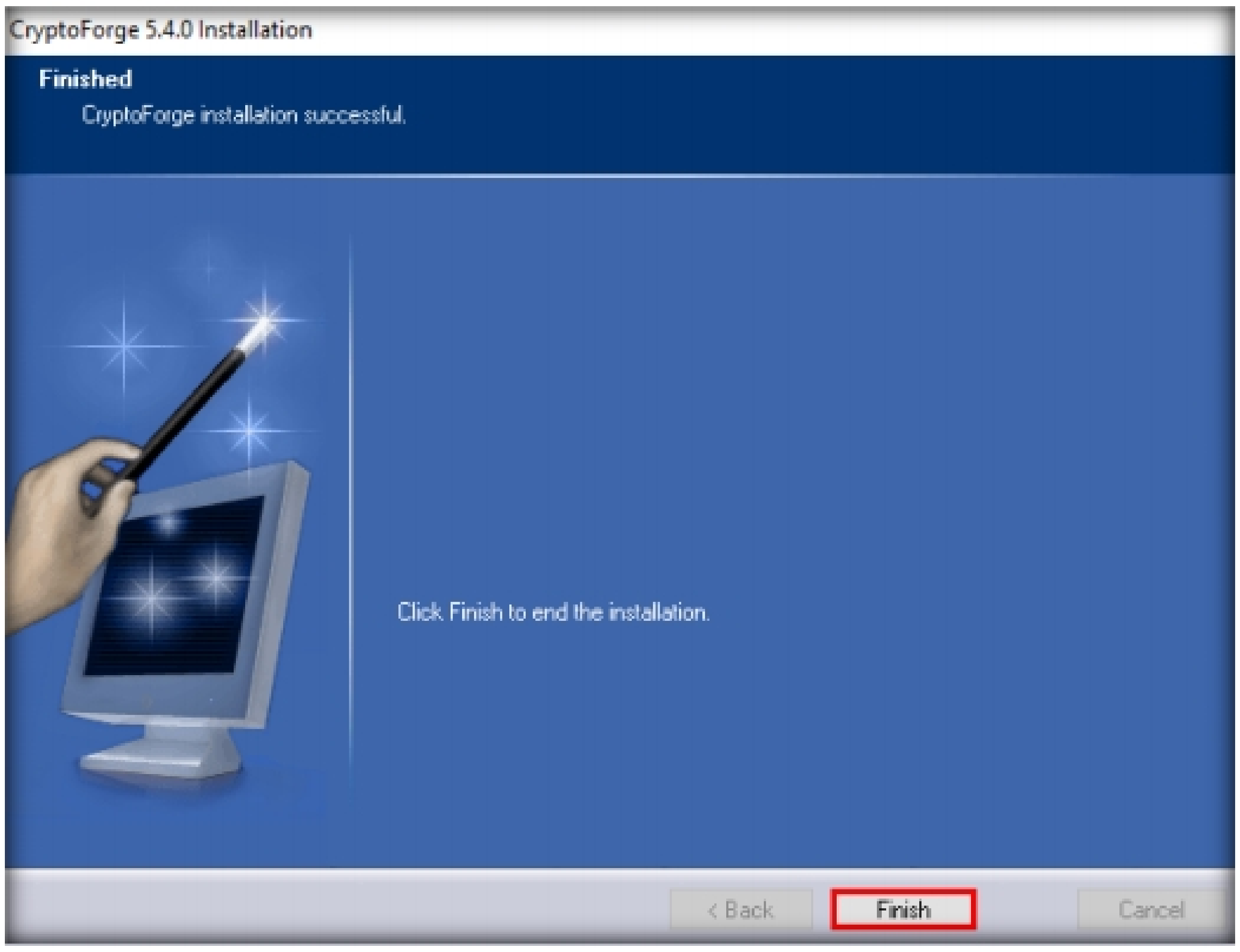
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Figure 1.4.1: CryptoForge Installation window

CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network—such as the Internet—and remain private. Later, the information can be decrypted into its original form.

4. Follow the installation steps to install the application using all default settings.

5. After completion of the installation, **CryptoForge installation successful** wizard appears; click **Finish**.



Finished

CryptoForge installation successful.

Click Finish to end the installation.

Figure 1.4.2: CryptoForge installation successful

6. Now, switch to the **Windows 10** virtual machine.
7. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, double-click **CryptoForge.exe**, and follow the steps to install the application using default settings.

TASK 4.2

Encrypt a File

8. Right-click the **Confidential.txt** file located at the same location (**E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**) and select **Encrypt** from the context menu.

Note: In this task, we are encrypting the **Confidential.txt** file, although you can encrypt any file of your choice.

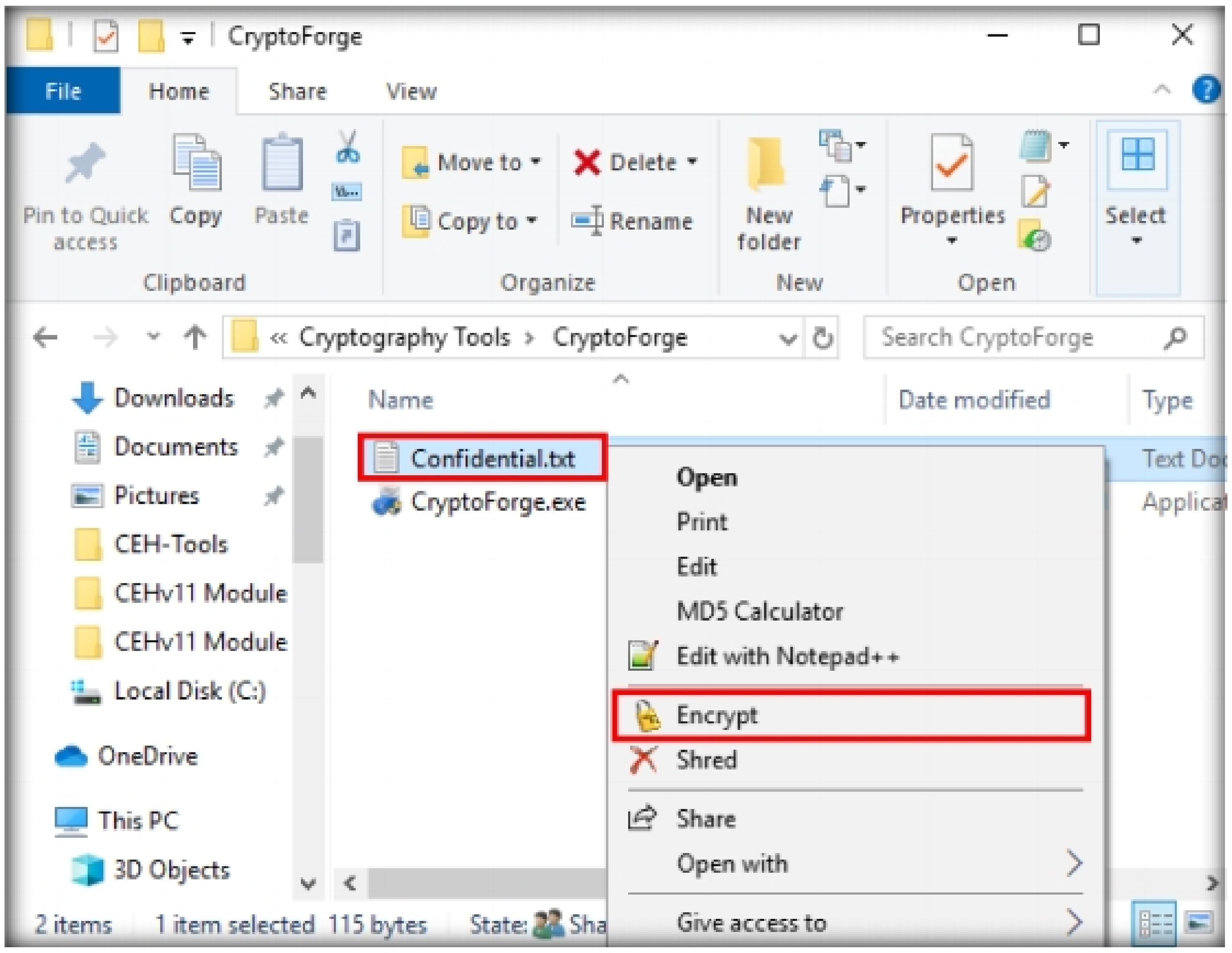
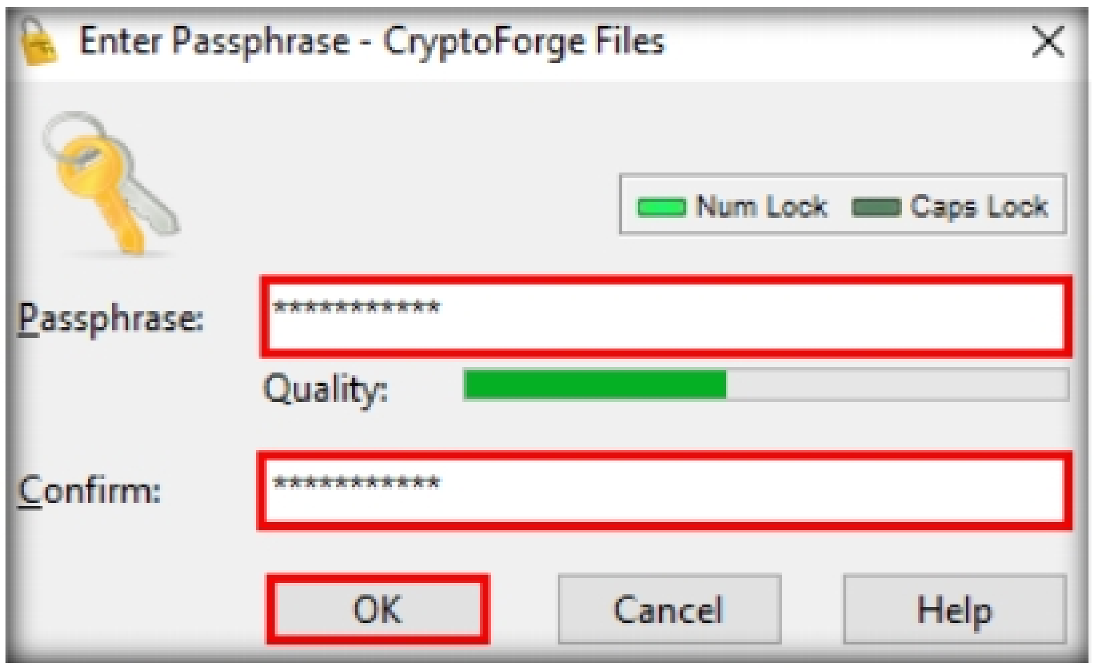

CryptoForge
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New
Properties
Open
Select
« Cryptography Tools › CryptoForge
Search CryptoForge
Downloads
Documents
Pictures
CEH-Tools
CEHv11 Module
CEHv11 Module
Local Disk (C:)
OneDrive
This PC
3D Objects
Name
Date modified
Type
Confidential.txt
CryptoForge.exe
Text Do
Applica
Open
Print
Edit
MD5 Calculator
Edit with Notepad++
Encrypt
Shred
Share
Open with
Give access to
2 items
1 item selected 115 bytes
State: Sha

Figure 1.4.3: Encrypting a File

9. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.


Enter Passphrase - CryptoForge Files
Num Lock
Caps Lock
Quality:
OK
Cancel
Help

Passphrase: ***********

Confirm: ***********

Figure 1.4.4: Enter Passphrase - CryptoForge Files Dialog-Box

10. Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

Note: No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.

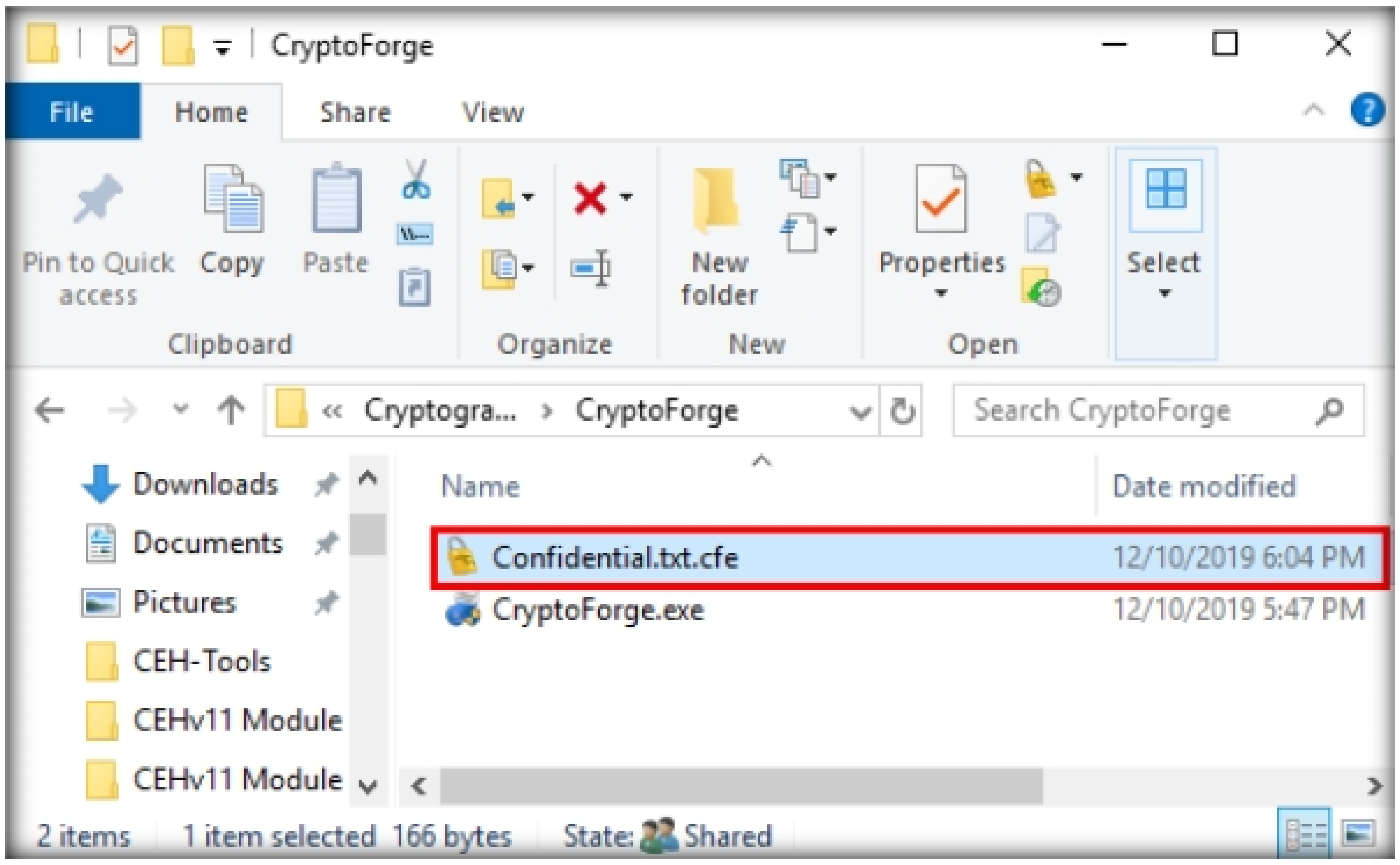

CryptoForge
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Organize
New folder
New
Properties
Open
Select
« Cryptogra... › CryptoForge
Search CryptoForge
Downloads
Documents
Pictures
CEH-Tools
CEHv11 Module
CEHv11 Module
Name
Date modified
Confidential.txt.cfe
12/10/2019 6:04 PM
CryptoForge.exe
12/10/2019 5:47 PM
2 items
1 item selected 166 bytes
State: Shared

Figure 1.4.5: File Encrypted

TASK 4.3

Decrypt the Encrypted File

11. Let us assume that you shared this file through a shared network drive.
12. Now, switch to the **Windows Server 2019** virtual machine and navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
13. Double-click the encrypted file to decrypt it and view its contents.

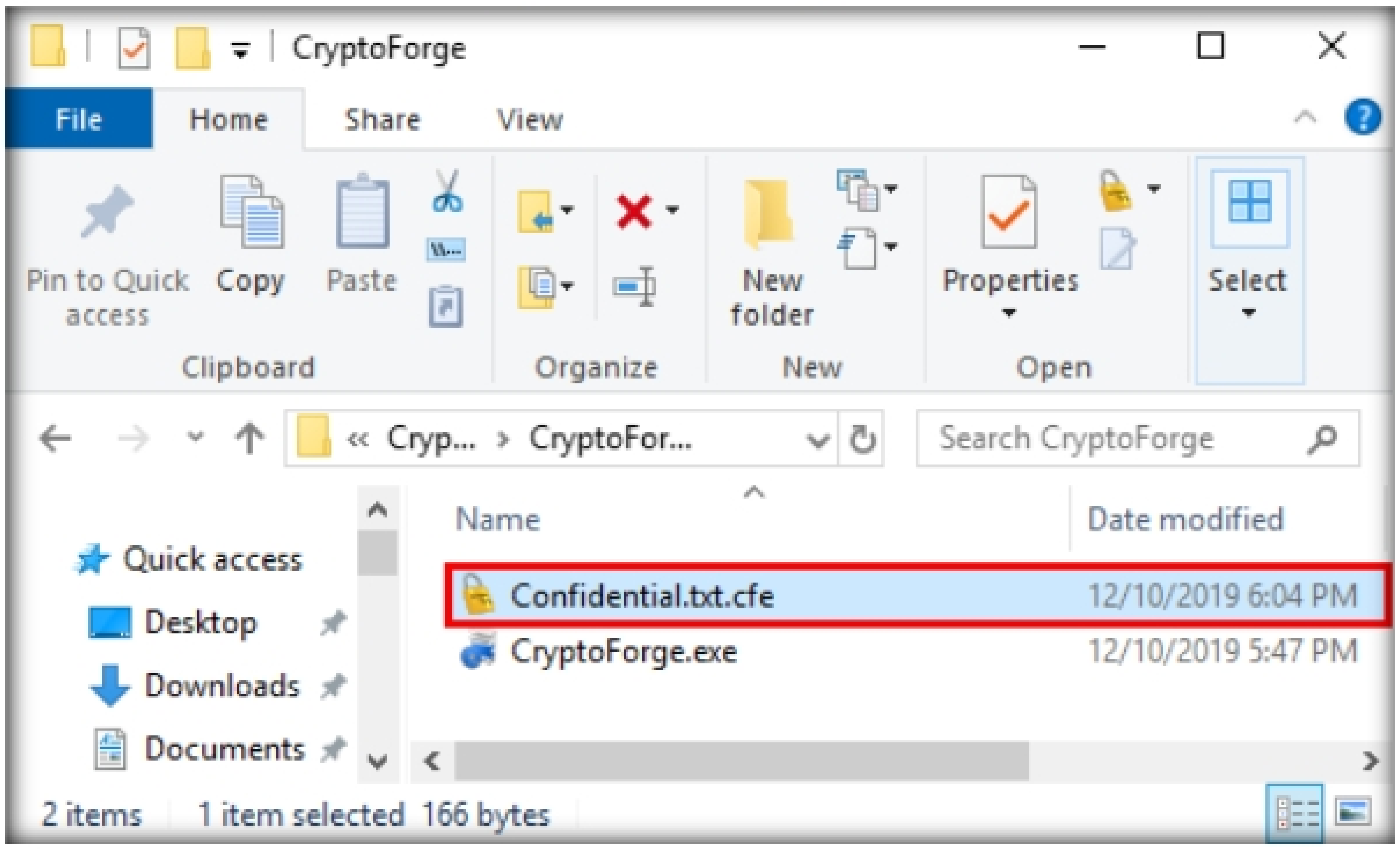
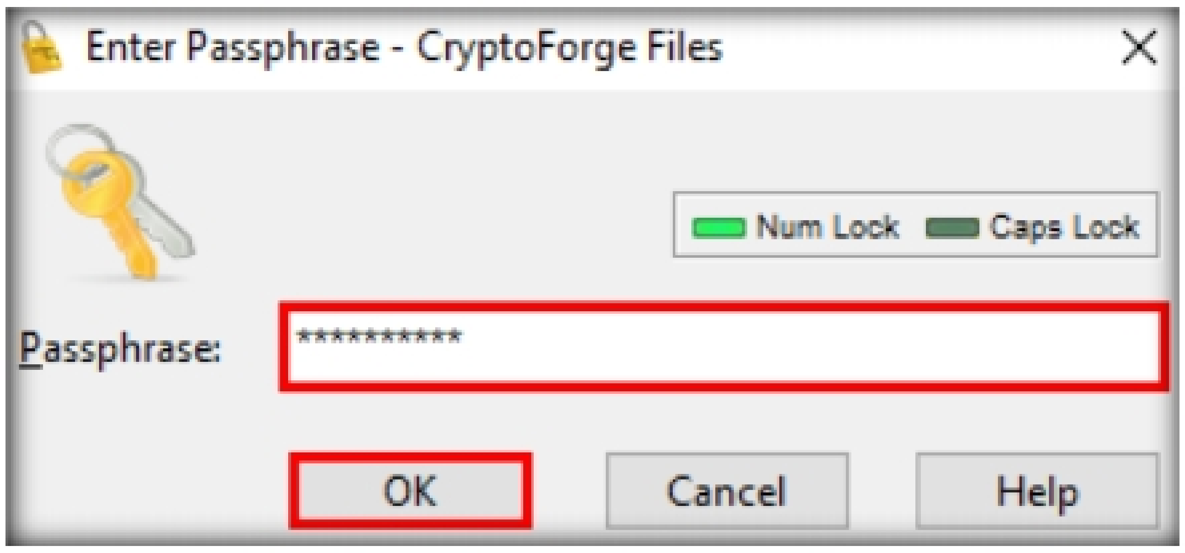

CryptoForge
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Organize
New folder
New
Properties
Open
Select
« Cryp... › CryptoFor...
Search CryptoForge
Quick access
Desktop
Downloads
Documents
Name
Date modified
Confidential.txt.cfe
12/10/2019 6:04 PM
CryptoForge.exe
12/10/2019 5:47 PM
2 items
1 item selected 166 bytes

Figure 1.4.6: Decrypted the Encrypted File

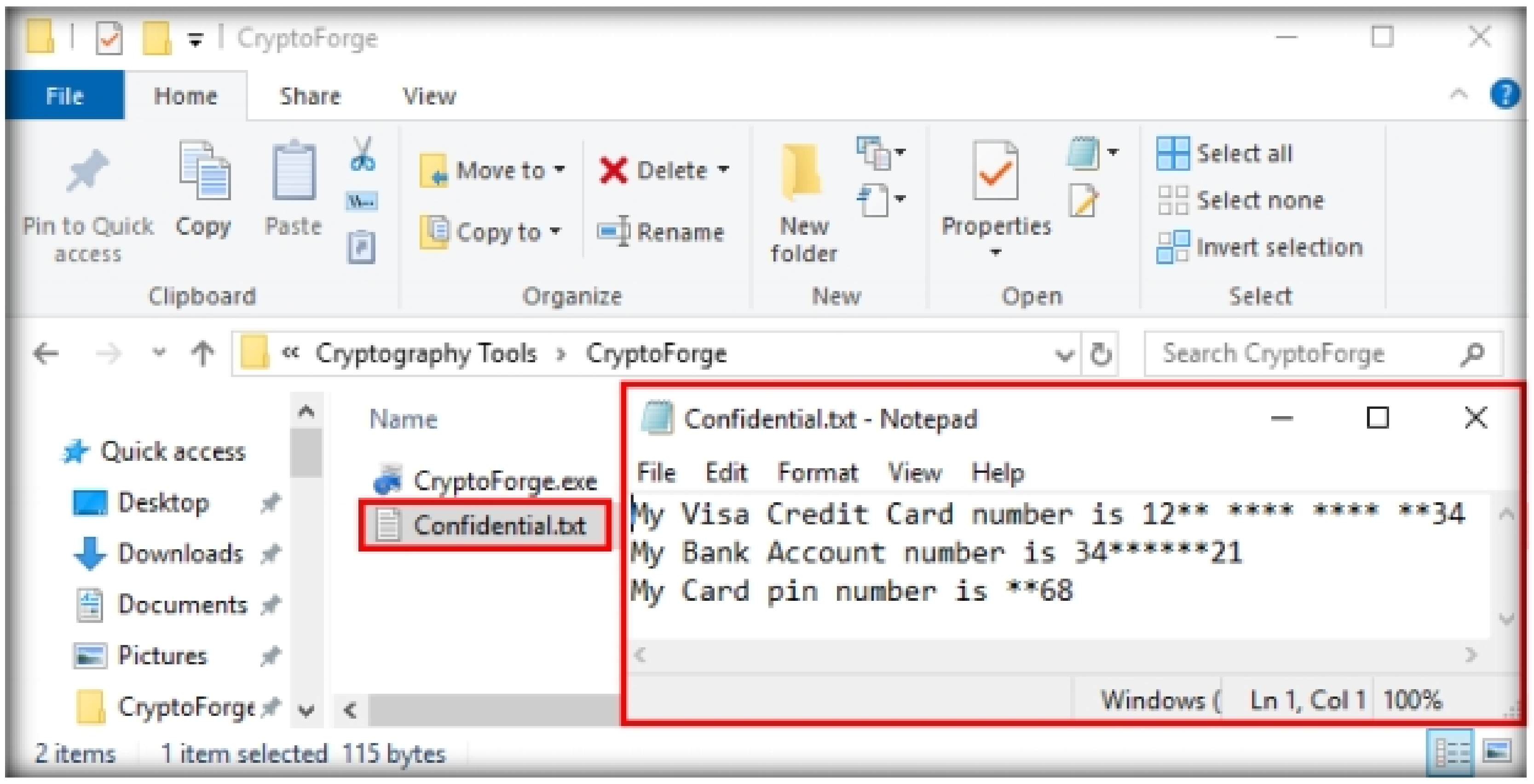
14. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#9** to encrypt the file and click **OK**.


Enter Passphrase - CryptoForge Files
Num Lock
Caps Lock
OK
Cancel
Help

Passphrase: ***********

Figure 1.4.7: Enter Passphrase - CryptoForge Files Dialog-Box

15. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.


CryptoForge
File
Home
Share
View
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
« Cryptography Tools › CryptoForge
Search CryptoForge
Quick access
Desktop
Downloads
Documents
Pictures
CryptoForge
Name
CryptoForge.exe
Confidential.txt
Confidential.txt - Notepad
File
Edit
Format
View
Help
Windows (
Ln 1, Col 1
100%
2 items
1 item selected 115 bytes

```
My Visa Credit Card number is 12** **** **** **34
My Bank Account number is 34******21
My Card pin number is **68
```

Figure 1.4.8: File Decrypted Successfully

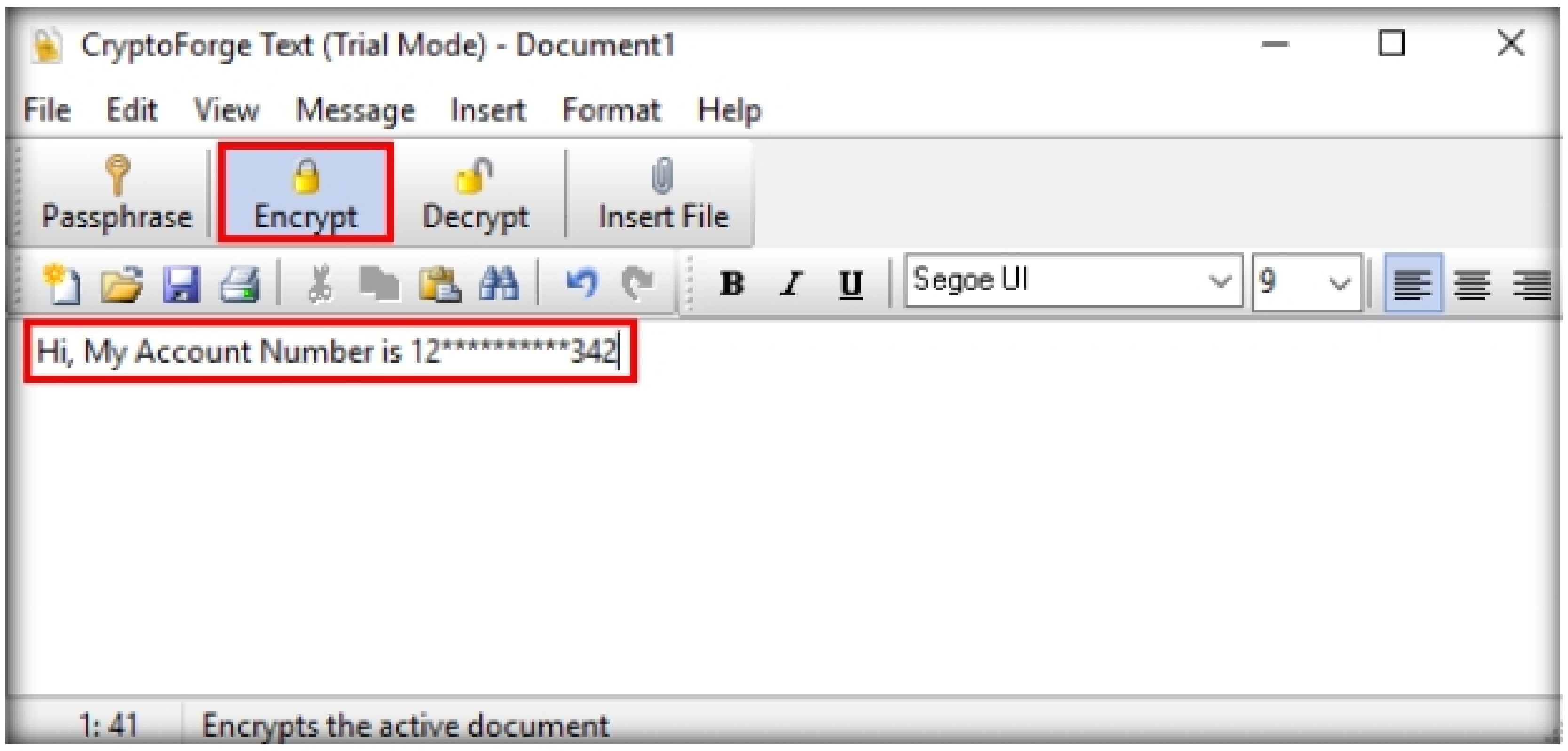
16. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.

TASK 4.4

Encrypt a Message

17. In the **Windows Server 2019** machine, click the **Start** icon present in the bottom-left corner of **Desktop** and click **CryptoForge Text** from the apps to launch the application.

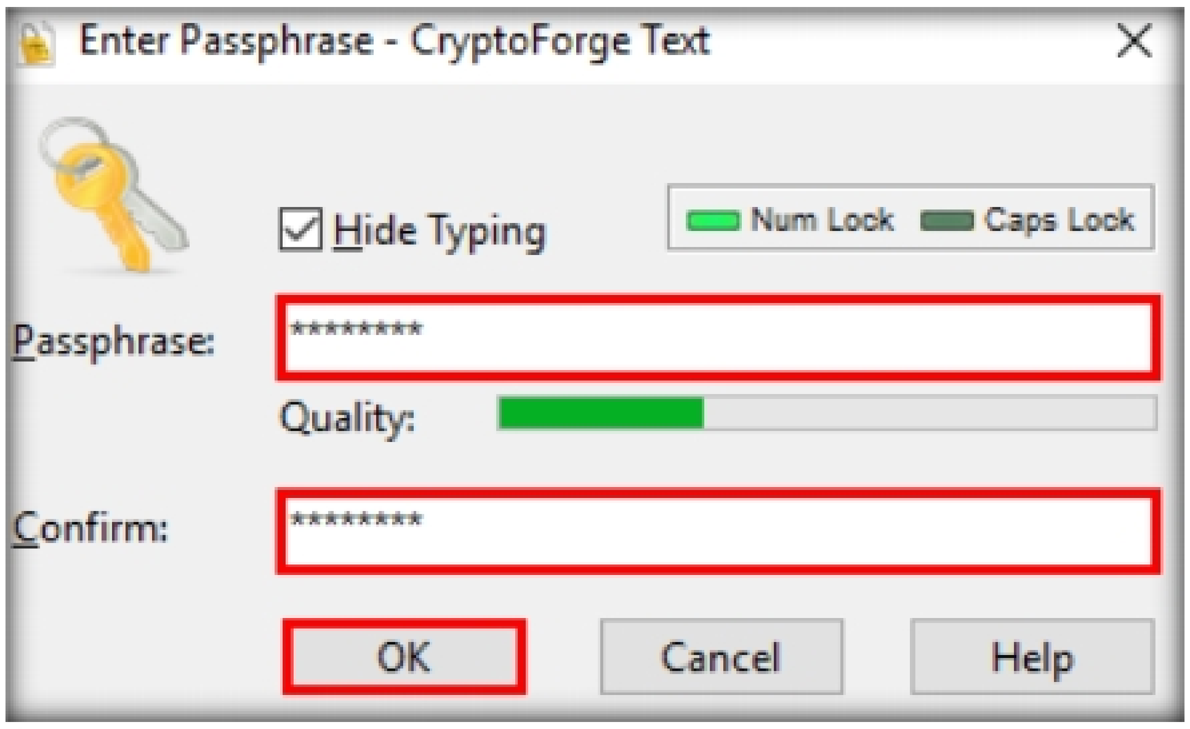
18. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.


CryptoForge Text (Trial Mode) - Document1
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Segoe UI
9
1: 41
Encrypts the active document

Hi, My Account Number is 12**********342

Figure 1.4.9: Encrypting a Text Message

19. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.

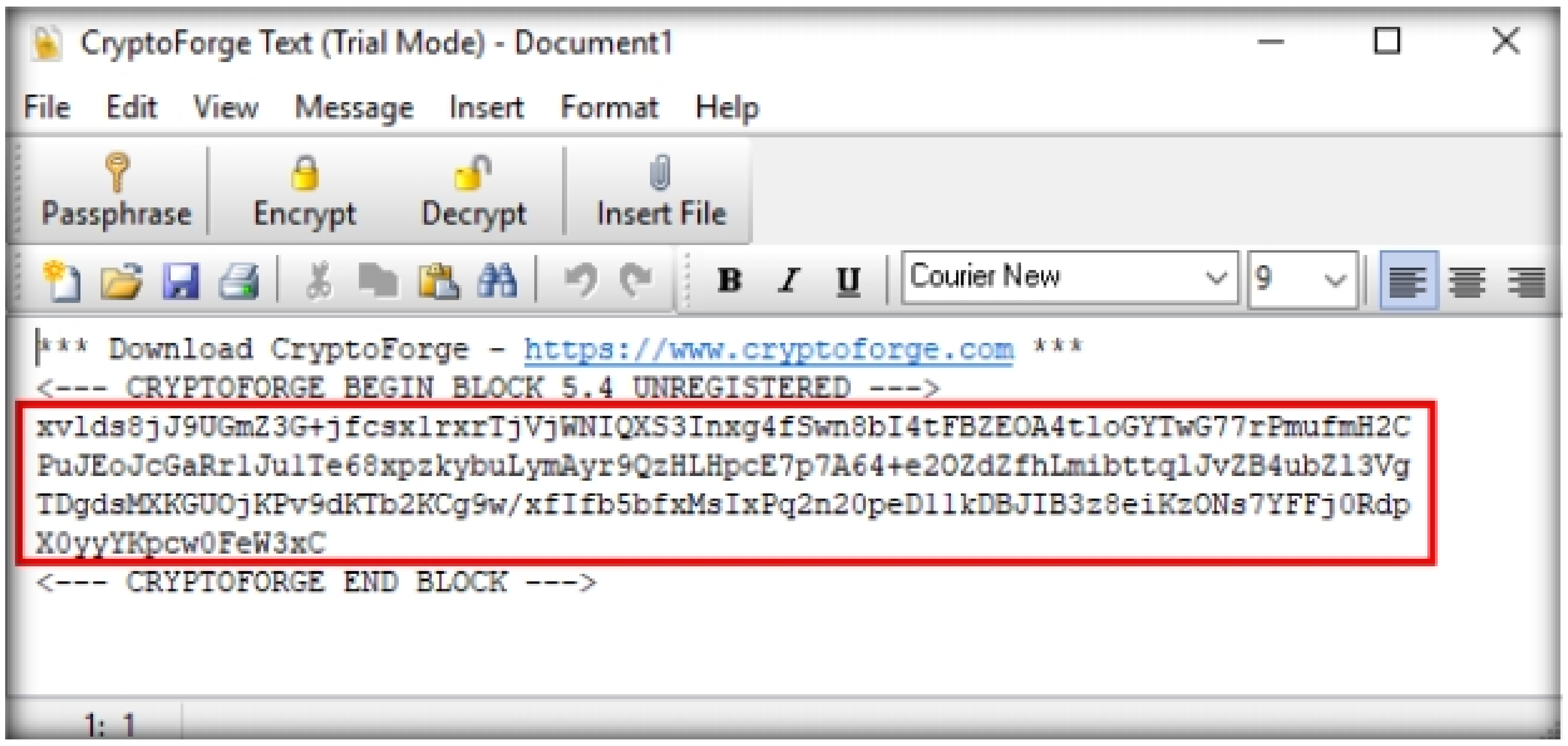

Enter Passphrase - CryptoForge Text
☑ Hide Typing
Num Lock
Caps Lock
Quality:
OK
Cancel
Help

Passphrase: *********

Confirm: *********

Figure 1.4.10: Enter Passphrase - CryptoForge Text Dialog-Box

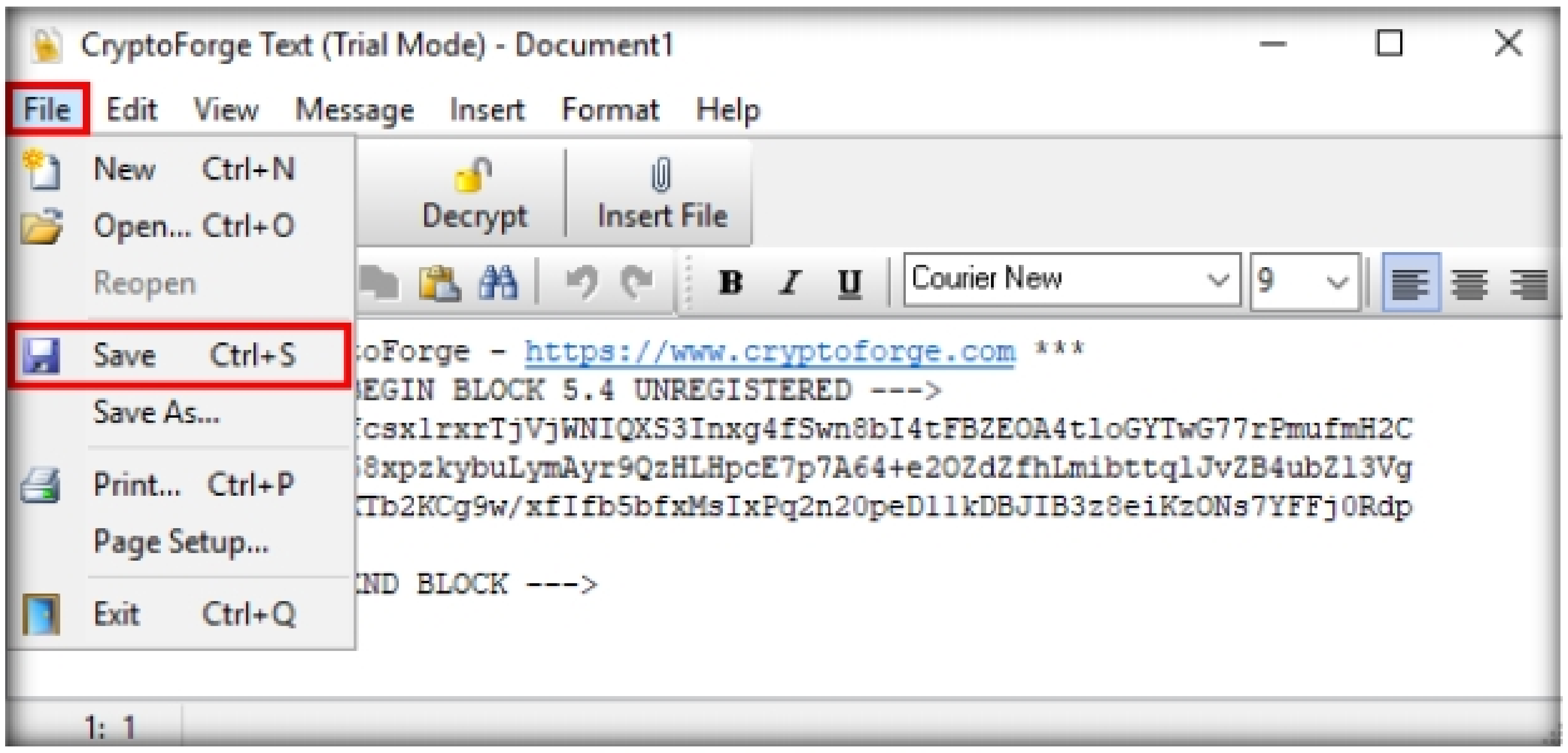
20. The message that you have typed will be encrypted, as shown in the screenshot.


CryptoForge Text (Trial Mode) - Document1
File Edit View Message Insert Format Help
Passphrase
Encrypt
Decrypt
Insert File
Courier New
9
1: 1

```
*** Download CryptoForge - https://www.cryptoforge.com ***
<--- CRYPTOFORGE BEGIN BLOCK 5.4 UNREGISTERED --->
xvlds8jJ9UGmZ3G+jfcsxlrxrTjVjWNIQXS3Inxg4fSwn8bI4tFBZEOA4tloGYTwG77rPmufmH2C
PuJEoJcGaRrlJulTe68xpzkybuLymAyr9QzHLHpcE7p7A64+e2OZdZfhLmibttqlJvZB4ubZl3Vg
TDgdsMXKGUOjKPv9dKTb2KCg9w/xfIfb5bfxMsIxPq2n20peDllkDBJIB3z8eiKzONs7YFFj0Rdp
X0yyYKpcw0FeW3xC
<--- CRYPTOFORGE END BLOCK --->
```

Figure 1.4.11: Encrypted Message

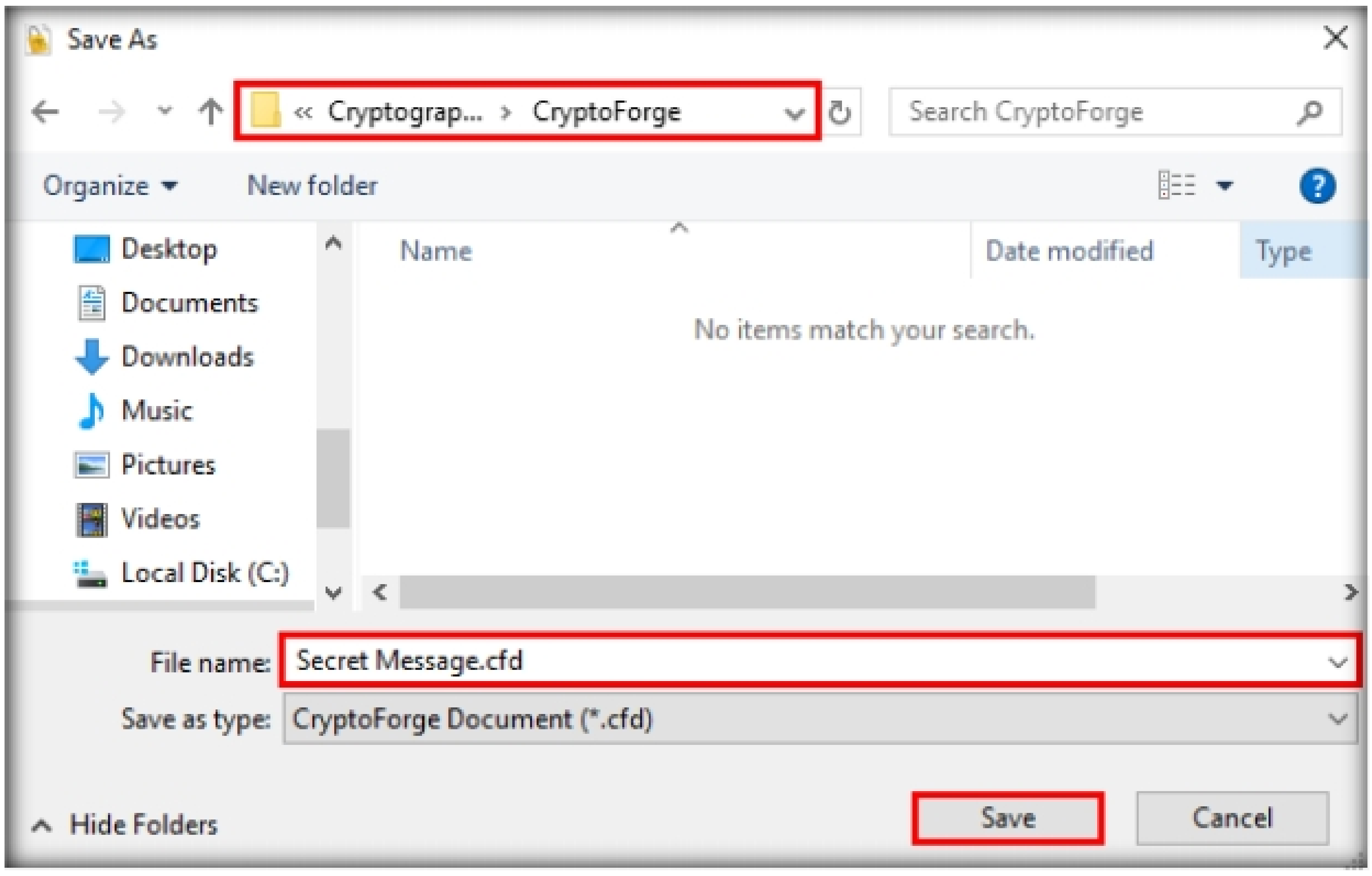
21. Now, you need to save the file. Click **File** in the menu bar and click **Save**.


CryptoForge Text (Trial Mode) - Document1
File
Edit
View
Message
Insert
Format
Help
New Ctrl+N
Open... Ctrl+O
Reopen
Save Ctrl+S
Save As...
Print... Ctrl+P
Page Setup...
Exit Ctrl+Q
Decrypt
Insert File
Courier New
9
1: 1

```
oForge - https://www.cryptoforge.com ***
EGIN BLOCK 5.4 UNREGISTERED --->
csxlrxrTjVjWNIQXS3Inxg4fSwn8bI4tFBZEOA4tloGYTwG77rPmufmH2C
8xpzkybuLymAyr9QzHLHpcE7p7A64+e2OZdZfhLmibttqlJvZB4ubZl3Vg
Tb2KCg9w/xfIfb5bfxMsIxPq2n20peDllkDBJIB3z8eiKzONs7YFFj0Rdp

ND BLOCK --->
```

Figure 1.4.12: Saving the File

22. The **Save As** window appears; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.


Save As
« Cryptograp... › CryptoForge
Search CryptoForge
Organize
New folder
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Name
Date modified
Type
No items match your search.
Hide Folders
Save
Cancel

File name: Secret Message.cfd

Save as type: CryptoForge Document (*.cfd)

Figure 1.4.13: Saving the File

23. Close the **CryptoForge Text** window.

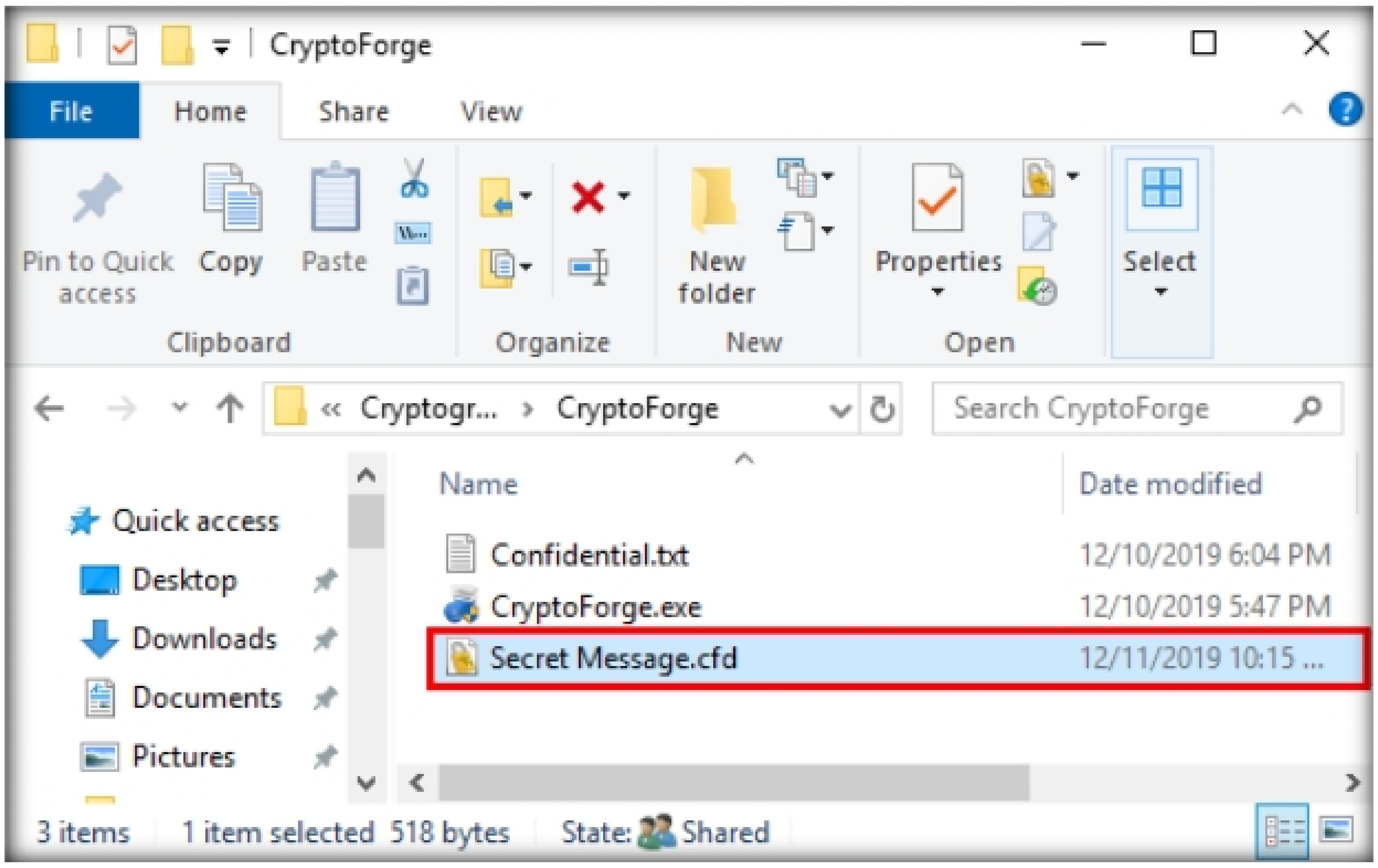
24. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.

TASK 4.5

Decrypt the Encrypted Message

25. Switch to the **Windows 10** virtual machine and navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\CryptoForge**.

26. You will observe the encrypted file in this location; double-click the file **Secret Message.cfd**.

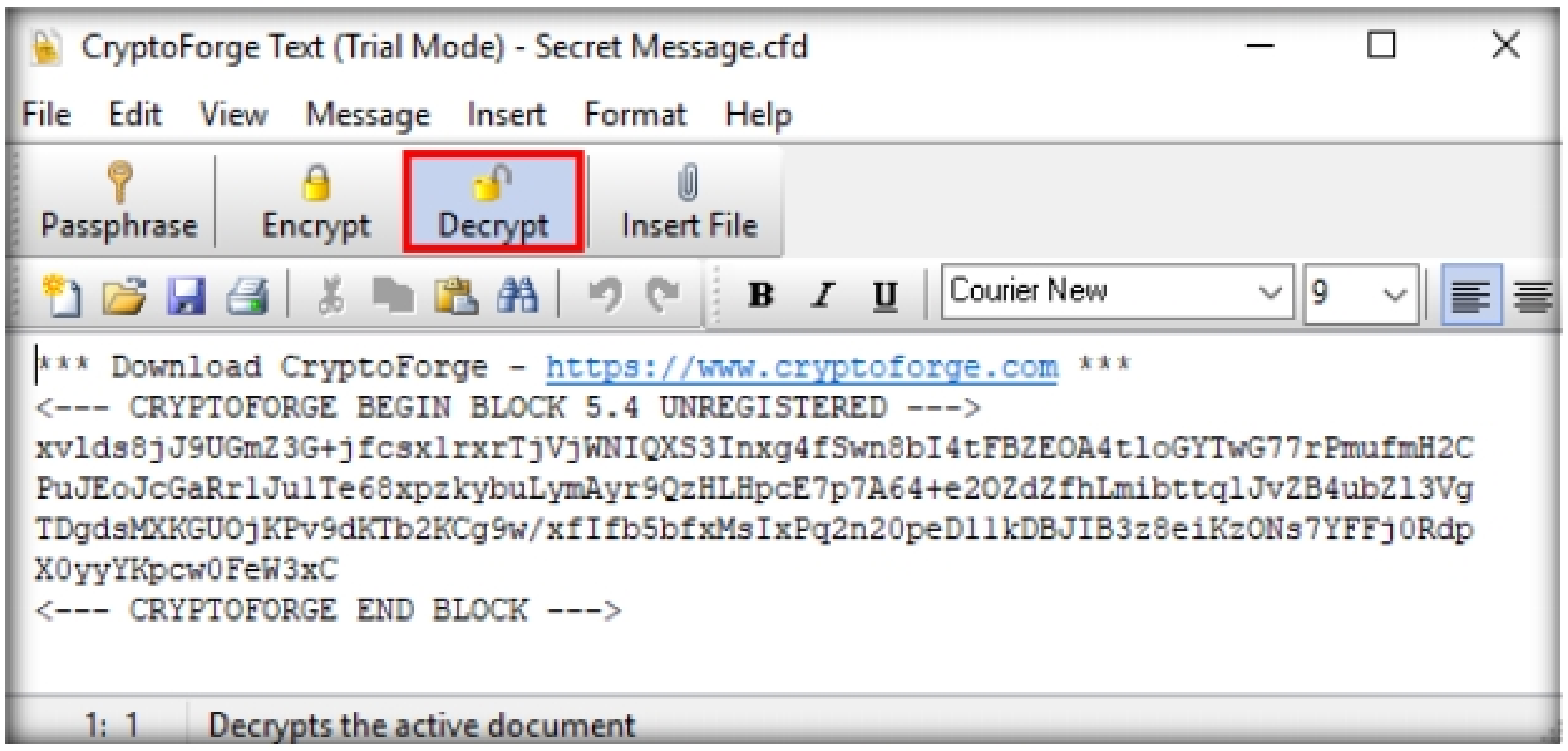

CryptoForge
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Organize
New folder
New
Properties
Open
Select
Cryptogr... › CryptoForge
Search CryptoForge
Quick access
Desktop
Downloads
Documents
Pictures

Name	Date modified
Confidential.txt	12/10/2019 6:04 PM
CryptoForge.exe	12/10/2019 5:47 PM
Secret Message.cfd	12/11/2019 10:15 ...

3 items   1 item selected 518 bytes   State: Shared

Figure 1.4.14: Viewing the Encrypted File

27. The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.

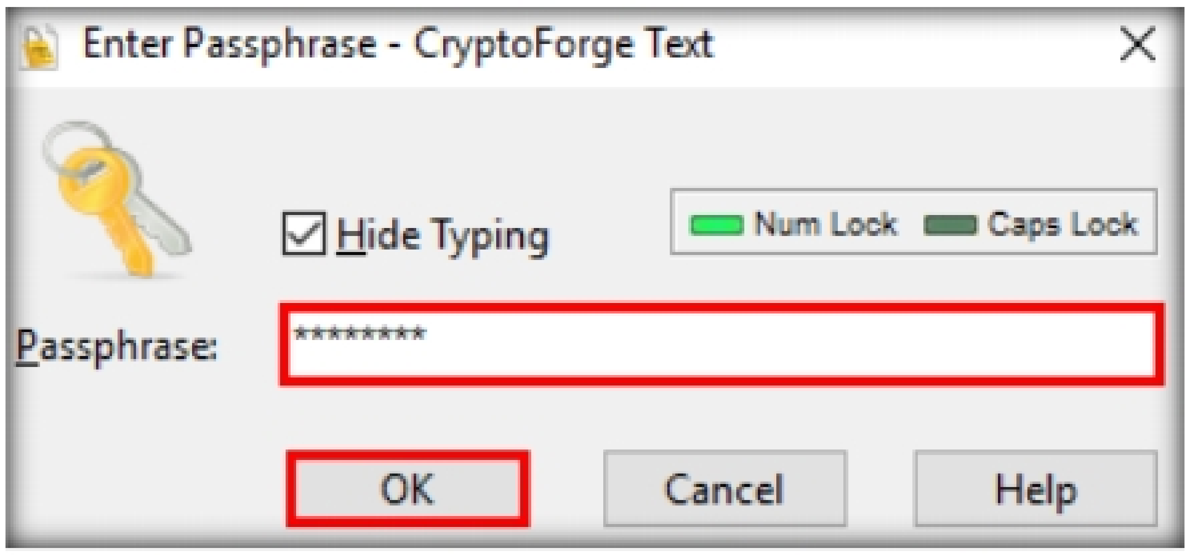

CryptoForge Text (Trial Mode) - Secret Message.cfd
File
Edit
View
Message
Insert
Format
Help
Passphrase
Encrypt
Decrypt
Insert File
Courier New
9

```
*** Download CryptoForge - https://www.cryptoforge.com ***
<--- CRYPTOFORGE BEGIN BLOCK 5.4 UNREGISTERED --->
xvlds8jJ9UGmZ3G+jfcsxlrxrTjVjWNIQXS3Inxg4fSwn8bI4tFBZEOA4tloGYTwG77rPmufmH2C
PuJEoJcGaRrlJulTe68xpzkybuLymAyr9QzHLHpcE7p7A64+e2OZdZfhLmibttqlJvZB4ubZl3Vg
TDgdsMXKGUOjKPv9dKTb2KCg9w/xfIfb5bfxMsIxPq2n20peDllkDBJIB3z8eiKzONs7YFFj0Rdp
X0yyYKpcw0FeW3xC
<--- CRYPTOFORGE END BLOCK --->
```

1: 1   Decrypts the active document

Figure 1.4.15: Decrypting the Encrypted File

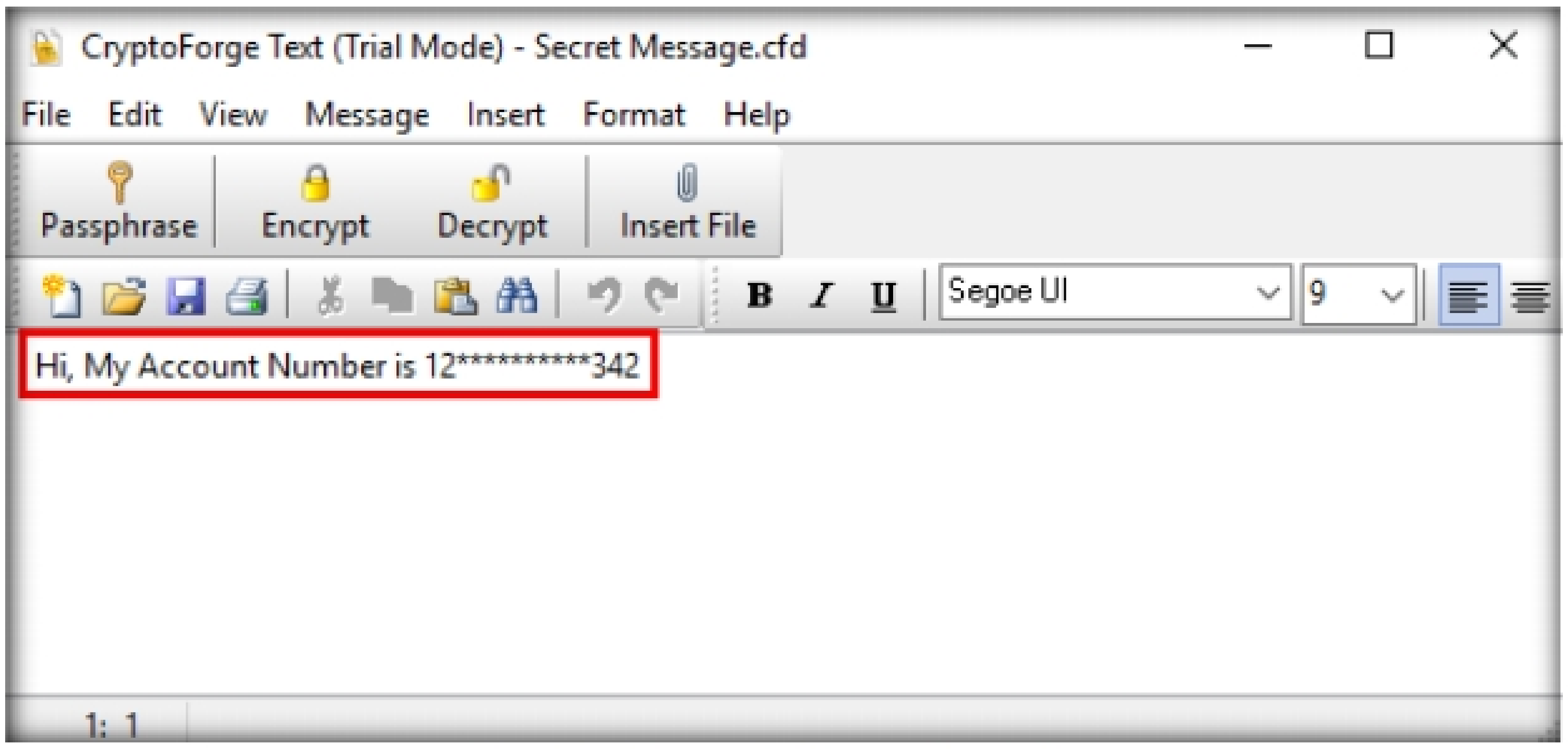
28. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#19** to decrypt the message in the **Passphrase** field and click **OK**.


Enter Passphrase - CryptoForge Text
☑ Hide Typing
Num Lock
Caps Lock
Passphrase:
OK
Cancel
Help

Passphrase: *********

Figure 1.4.16: Enter Passphrase - CryptoForge Text Dialog-Box

29. The **CryptoForge Text** window appears, displaying the message in plain-text format, as shown in the screenshot.


CryptoForge Text (Trial Mode) - Secret Message.cfd
File
Edit
View
Message
Insert
Format
Help
Passphrase
Encrypt
Decrypt
Insert File
Segoe UI
9
1: 1

Hi, My Account Number is 12**********342

Figure 1.4.17: Message Decrypted Successfully

Note: In real-time, you may share sensitive information through email by encrypting data using CryptoForge.

30. This concludes the demonstration of performing file and text message encryption using CryptoForge.
31. Close all open windows and document all the acquired information.
32. Turn off the **Windows Server 2019** virtual machine.

TASK 5

Perform File Encryption using Advanced Encryption Package

Here, we will use the Advanced Encryption Package tool to perform file encryption.

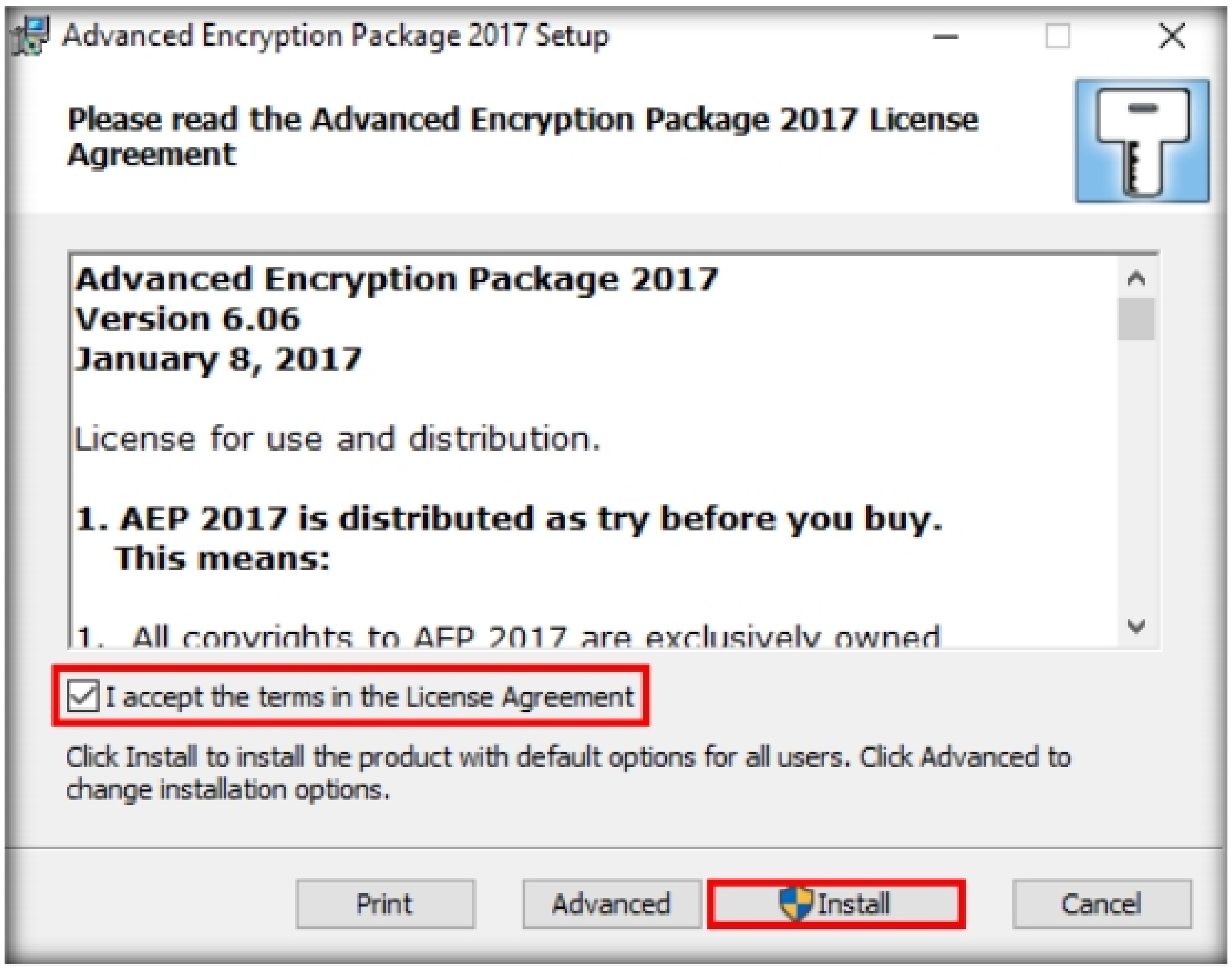
TASK 5.1

Install Advanced Encryption Package

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package** and double-click **aep.msi**.
2. **Windows Installer** initializes and the **Advanced Encryption Package Setup** window appears; click the **I accept the terms in the License Agreement** checkbox; then, click **Install**.

Advanced Encryption Package is a file encryption software for Windows used for secure file transfer, batch file encryption, and encrypted backups. It supports file and/or text encryption, performs secure file deletion, and creates an encrypted self-extracting file to send as an email attachment.

Note: If a **User Account Control** pop-up appears, click **Yes**.



Please read the Advanced Encryption Package 2017 License Agreement

Advanced Encryption Package 2017
Version 6.06
January 8, 2017

License for use and distribution.

1. AEP 2017 is distributed as try before you buy.
This means:

1. All copyrights to AEP 2017 are exclusively owned

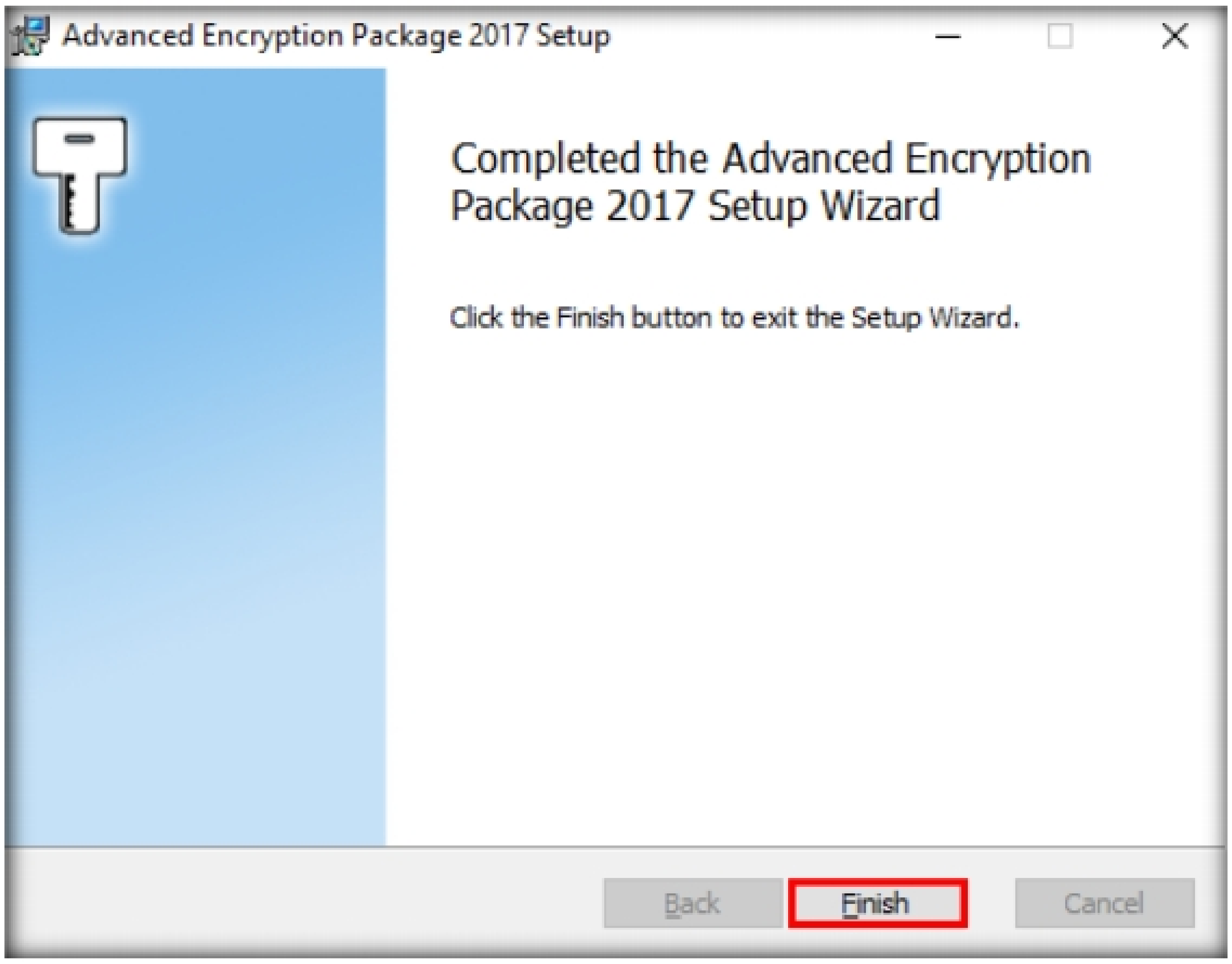
☑ I accept the terms in the License Agreement

Click Install to install the product with default options for all users. Click Advanced to change installation options.

Figure 1.5.1: Advanced Encryption Package Setup window

3. Follow the steps to install the application with default settings.

4. After the completion of the installation, **Completed the Advanced Encryption Package Setup Wizard** appears; then, click **Finish**.



Completed the Advanced Encryption Package 2017 Setup Wizard

Click the Finish button to exit the Setup Wizard.

Figure 1.5.2: Advanced Encryption Package Setup window

5. Now, click the **Start** icon from the bottom-left corner of **Desktop**; and from the list of **Recently added** applications, click **Advanced Encryption Package 2017** to launch the application.

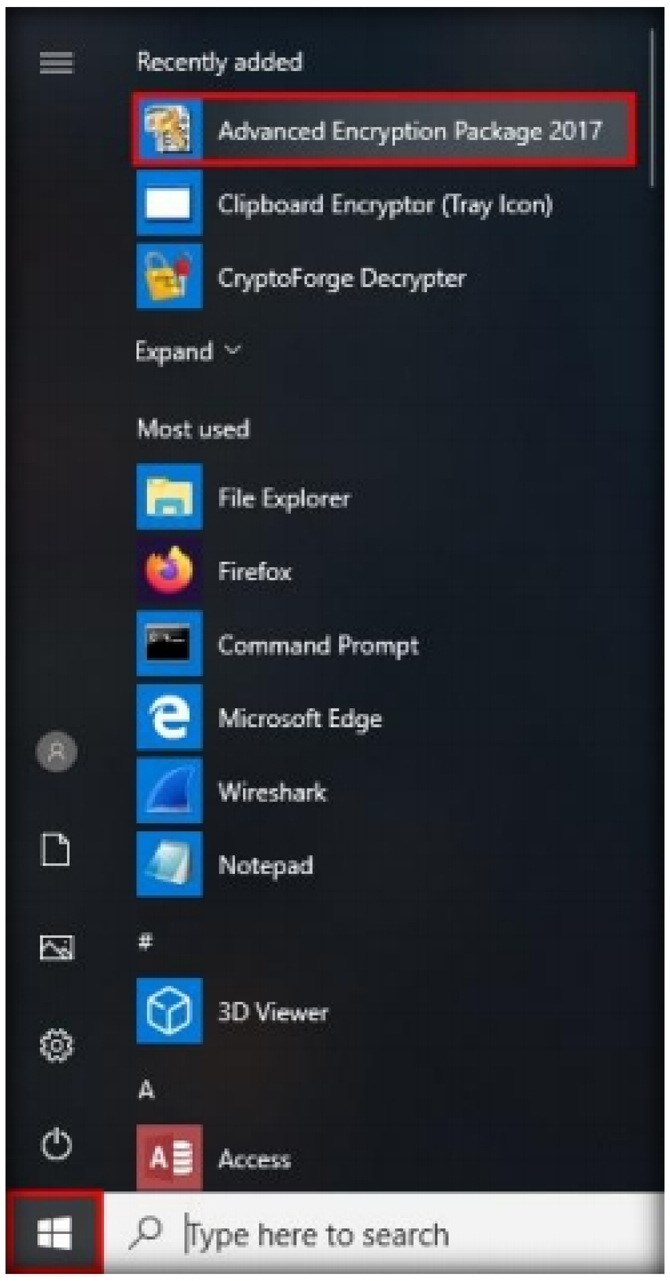

Recently added
Advanced Encryption Package 2017
Clipboard Encryptor (Tray Icon)
CryptoForge Decrypter
Expand
Most used
File Explorer
Firefox
Command Prompt
Microsoft Edge
Wireshark
Notepad
#
3D Viewer
A
Access
Type here to search

Figure 1.5.3: Launching Advanced Encryption Package application from the Apps screen

6. The **Advanced Encryption Package - License Manager** window appears. Under the **License Manager** section, select the **Start free 30-day trial** radio button and click **Next**.

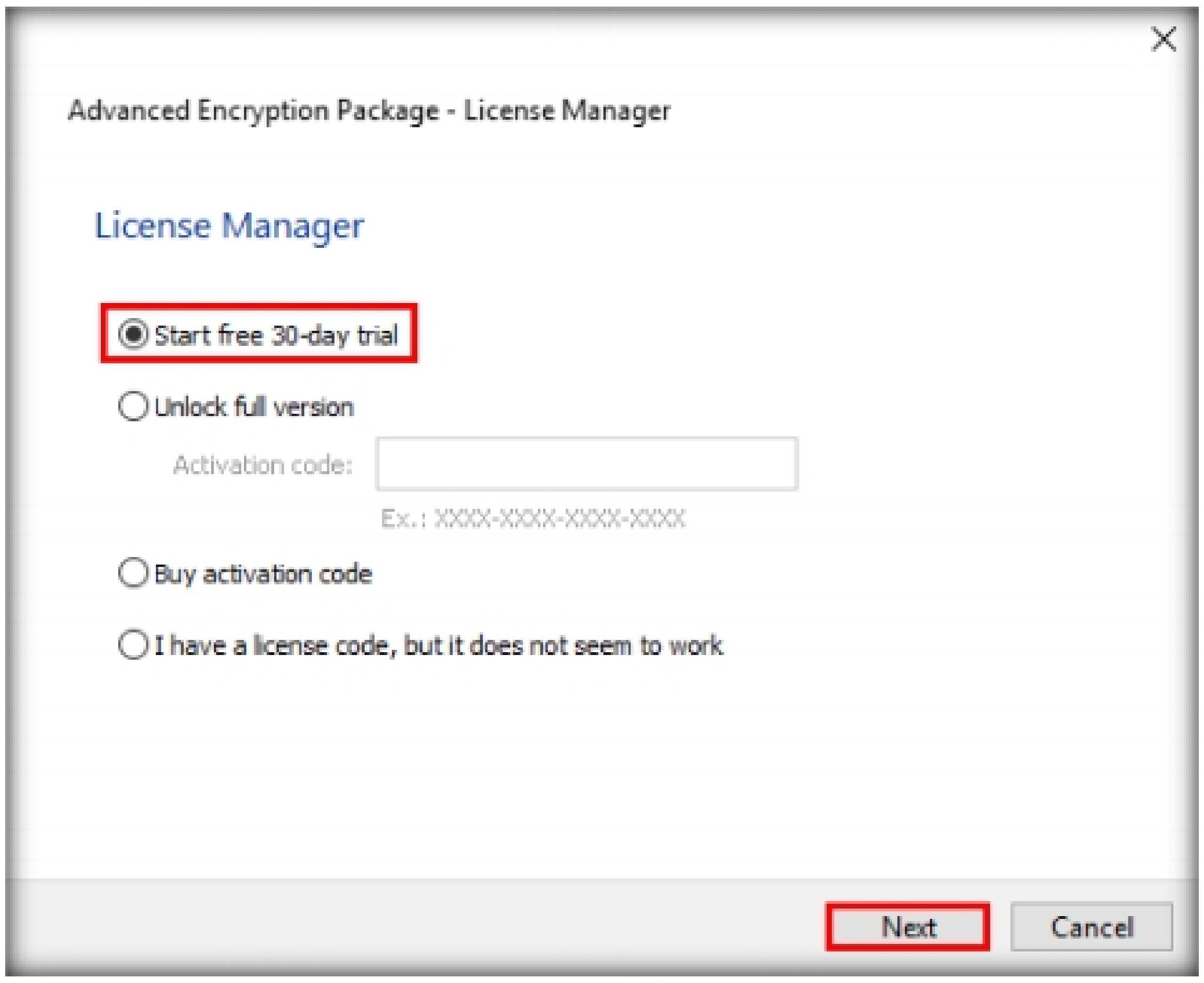
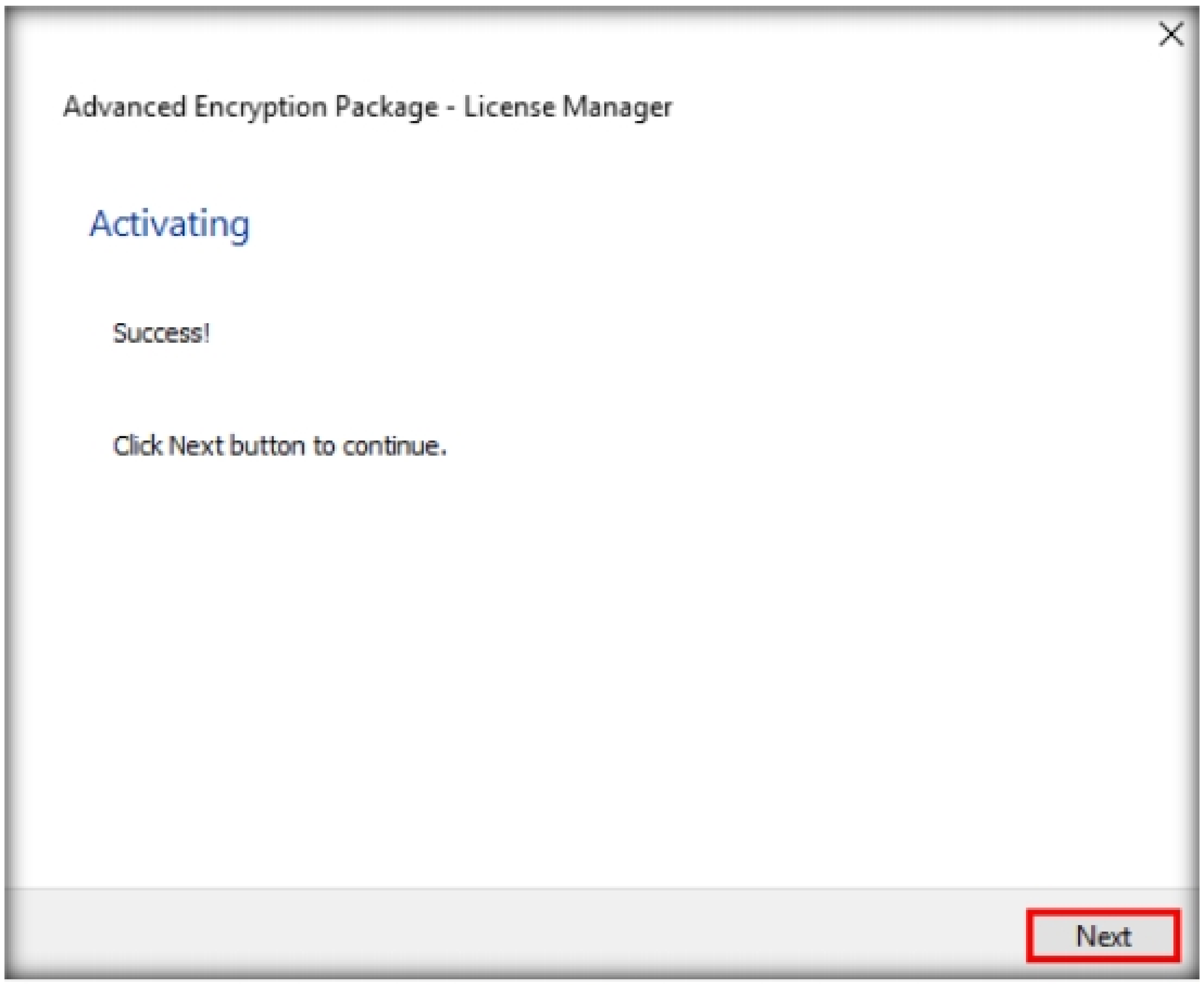

Advanced Encryption Package - License Manager
License Manager
● Start free 30-day trial
○ Unlock full version
Activation code:
Ex.: XXXX-XXXX-XXXX-XXXX
○ Buy activation code
○ I have a license code, but it does not seem to work
Next
Cancel

Figure 1.5.4: License Manager window

7. The **Activating** step appears displaying a **Success!** message; then, click **Next**.



Advanced Encryption Package - License Manager

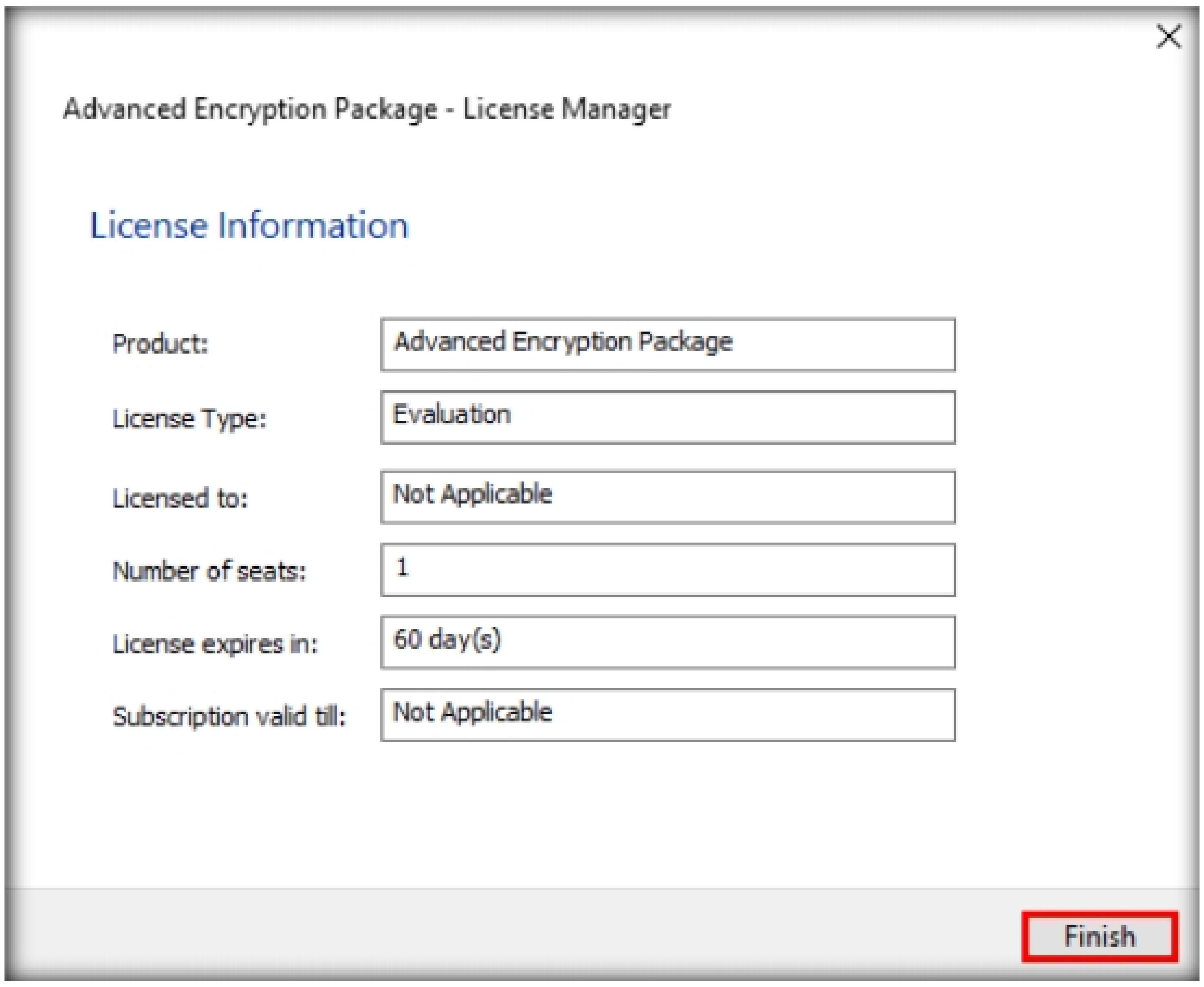
Activating

Success!

Click Next button to continue.

Figure 1.5.5: Activation Window

8. Leave all options set to default in the **License Information** step and click **Finish**.



Advanced Encryption Package - License Manager

License Information

Product:	Advanced Encryption Package
License Type:	Evaluation
Licensed to:	Not Applicable
Number of seats:	1
License expires in:	60 day(s)
Subscription valid till:	Not Applicable

Figure 1.5.6: License Information section

9. The **Advanced Encryption Package** main window appears, as shown in the screenshot.

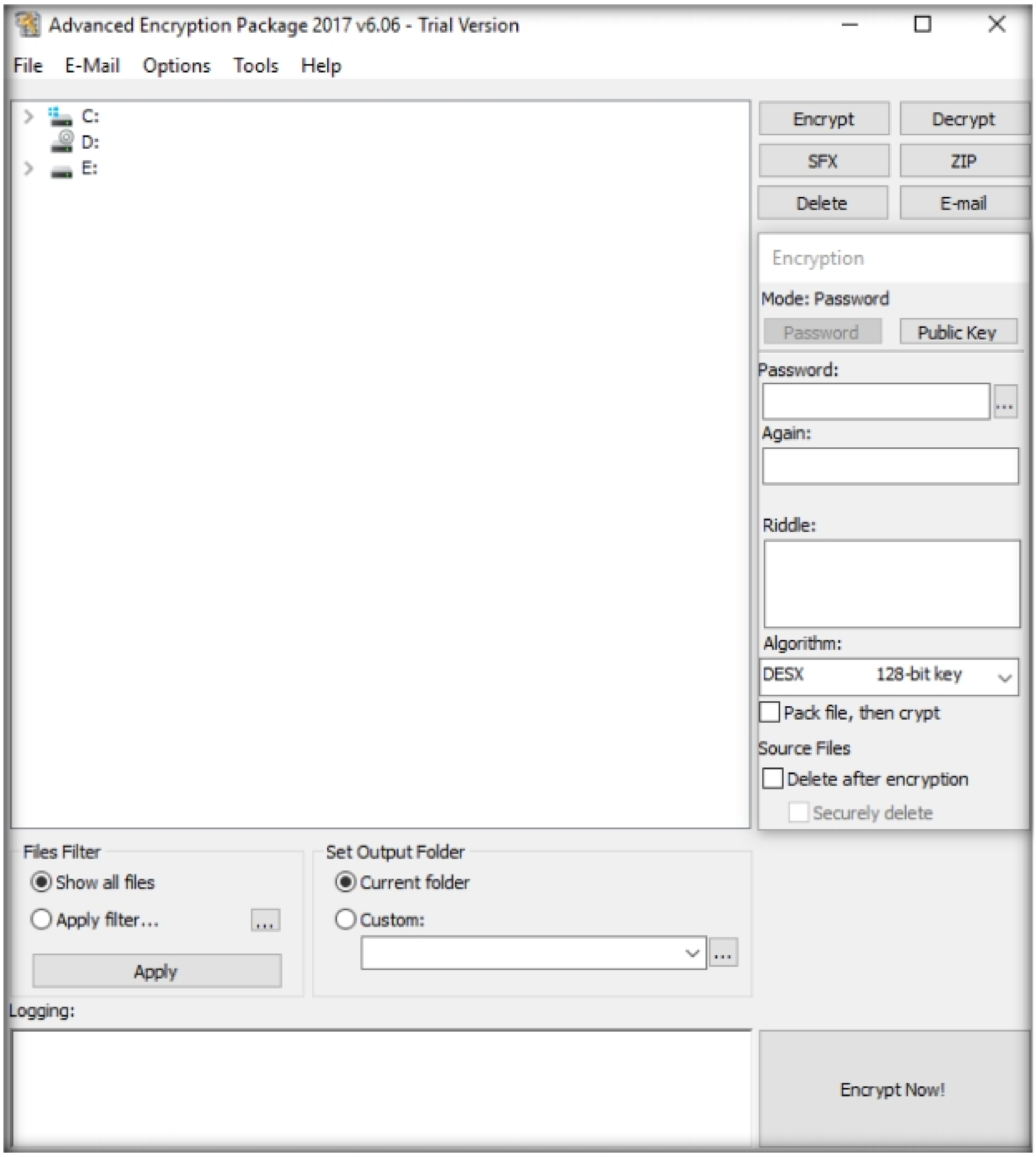
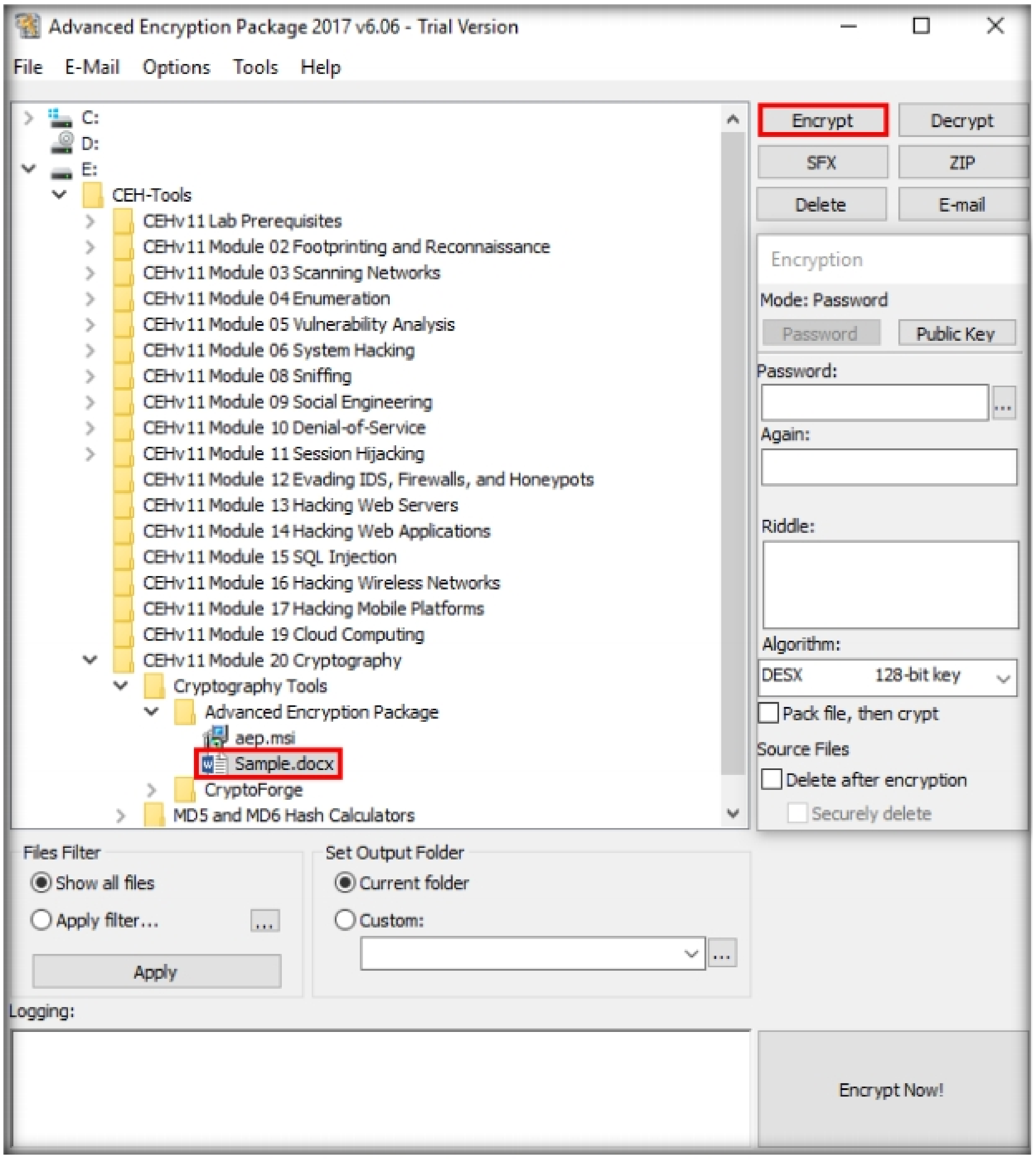

Advanced Encryption Package 2017 v6.06 - Trial Version
File
E-Mail
Options
Tools
Help
C:
D:
E:
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Encryption
Mode: Password
Password
Public Key
Password:
Again:
Riddle:
Algorithm:
DESX 128-bit key
☐ Pack file, then crypt
Source Files
☐ Delete after encryption
☐ Securely delete
Files Filter
● Show all files
○ Apply filter...
Apply
Set Output Folder
● Current folder
○ Custom:
Logging:
Encrypt Now!

Figure 1.5.7: License Information section

TASK 5.2

Encrypt a File

10. In the **Advanced Encryption Package** window, expand **E:** drive and navigate to **CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**. Select the **Sample.docx** file located in the given location and click **Encrypt** in the toolbar


Advanced Encryption Package 2017 v6.06 - Trial Version
File
E-Mail
Options
Tools
Help
C:
D:
E:
CEH-Tools
CEHv11 Lab Prerequisites
CEHv11 Module 02 Footprinting and Reconnaissance
CEHv11 Module 03 Scanning Networks
CEHv11 Module 04 Enumeration
CEHv11 Module 05 Vulnerability Analysis
CEHv11 Module 06 System Hacking
CEHv11 Module 08 Sniffing
CEHv11 Module 09 Social Engineering
CEHv11 Module 10 Denial-of-Service
CEHv11 Module 11 Session Hijacking
CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 15 SQL Injection
CEHv11 Module 16 Hacking Wireless Networks
CEHv11 Module 17 Hacking Mobile Platforms
CEHv11 Module 19 Cloud Computing
CEHv11 Module 20 Cryptography
Cryptography Tools
Advanced Encryption Package
aep.msi
Sample.docx
CryptoForge
MD5 and MD6 Hash Calculators
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Encryption
Password
Public Key
Password:
Again:
Riddle:
Algorithm:
Source Files
Files Filter
Apply filter...
Apply
Set Output Folder
Custom:
Logging:
Encrypt Now!

Mode: Password

Algorithm: DESX 128-bit key

☐ Pack file, then crypt

☐ Delete after encryption

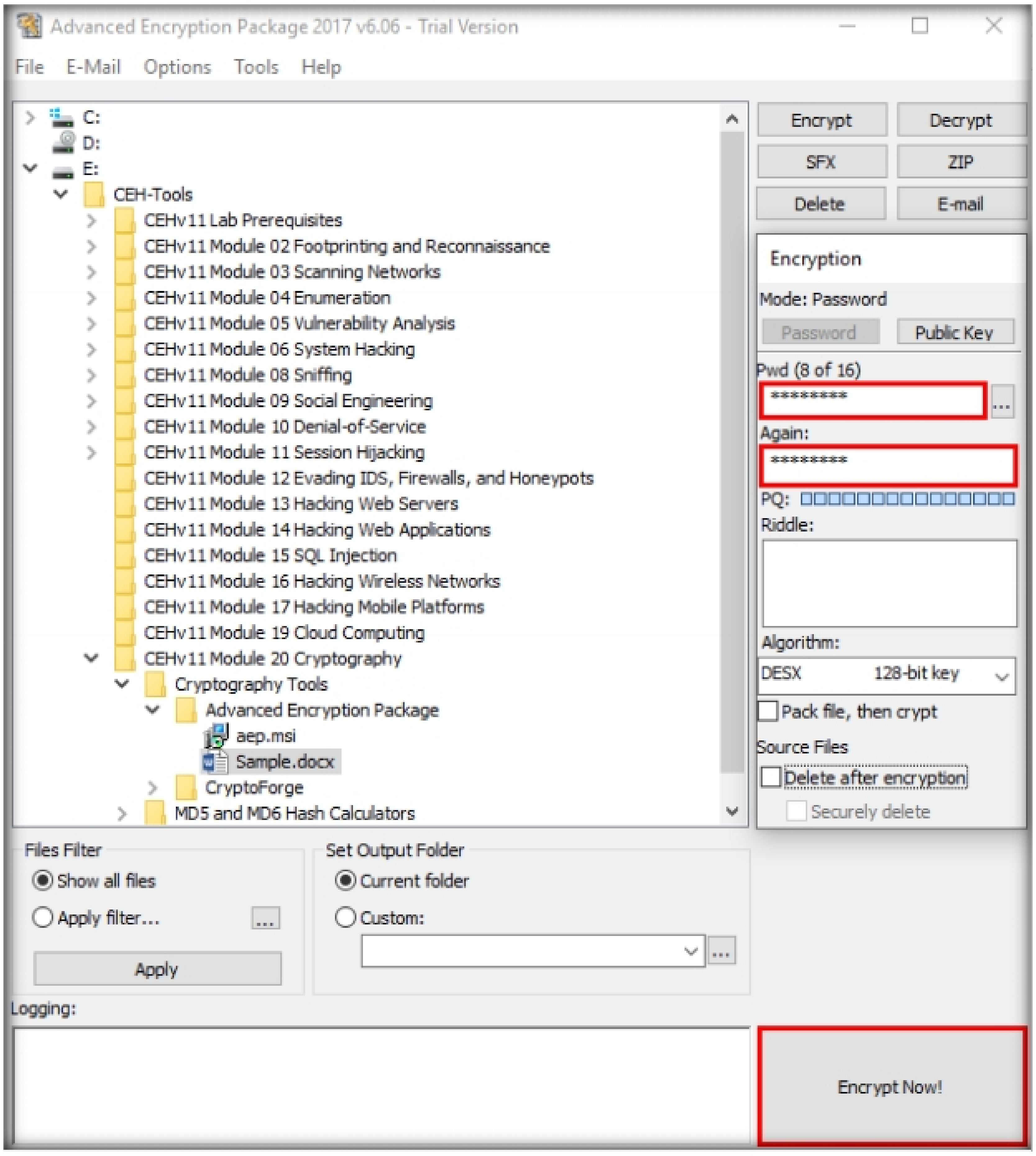
☐ Securely delete

● Show all files

● Current folder

Figure 1.5.8: Main window of Advance Encryption Package

11. You need to provide a password for encryption. In the right-hand pane, enter the password into the **Pwd** field, retype it in the **Again** field, and click **Encrypt Now!** button (Here, the password provided is **test@123**).


Advanced Encryption Package 2017 v6.06 - Trial Version
File
E-Mail
Options
Tools
Help
C:
D:
E:
CEH-Tools
CEHv11 Lab Prerequisites
CEHv11 Module 02 Footprinting and Reconnaissance
CEHv11 Module 03 Scanning Networks
CEHv11 Module 04 Enumeration
CEHv11 Module 05 Vulnerability Analysis
CEHv11 Module 06 System Hacking
CEHv11 Module 08 Sniffing
CEHv11 Module 09 Social Engineering
CEHv11 Module 10 Denial-of-Service
CEHv11 Module 11 Session Hijacking
CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 15 SQL Injection
CEHv11 Module 16 Hacking Wireless Networks
CEHv11 Module 17 Hacking Mobile Platforms
CEHv11 Module 19 Cloud Computing
CEHv11 Module 20 Cryptography
Cryptography Tools
Advanced Encryption Package
aep.msi
Sample.docx
CryptoForge
MD5 and MD6 Hash Calculators
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Encryption
Password
Public Key
Riddle:
Files Filter
Apply filter...
Apply
Set Output Folder
Logging:
Encrypt Now!

Mode: Password

Pwd (8 of 16): ********

Again: ********

PQ: □□□□□□□□□□□□□□□

Algorithm: DESX 128-bit key

☐ Pack file, then crypt

Source Files

☐ Delete after encryption

☐ Securely delete

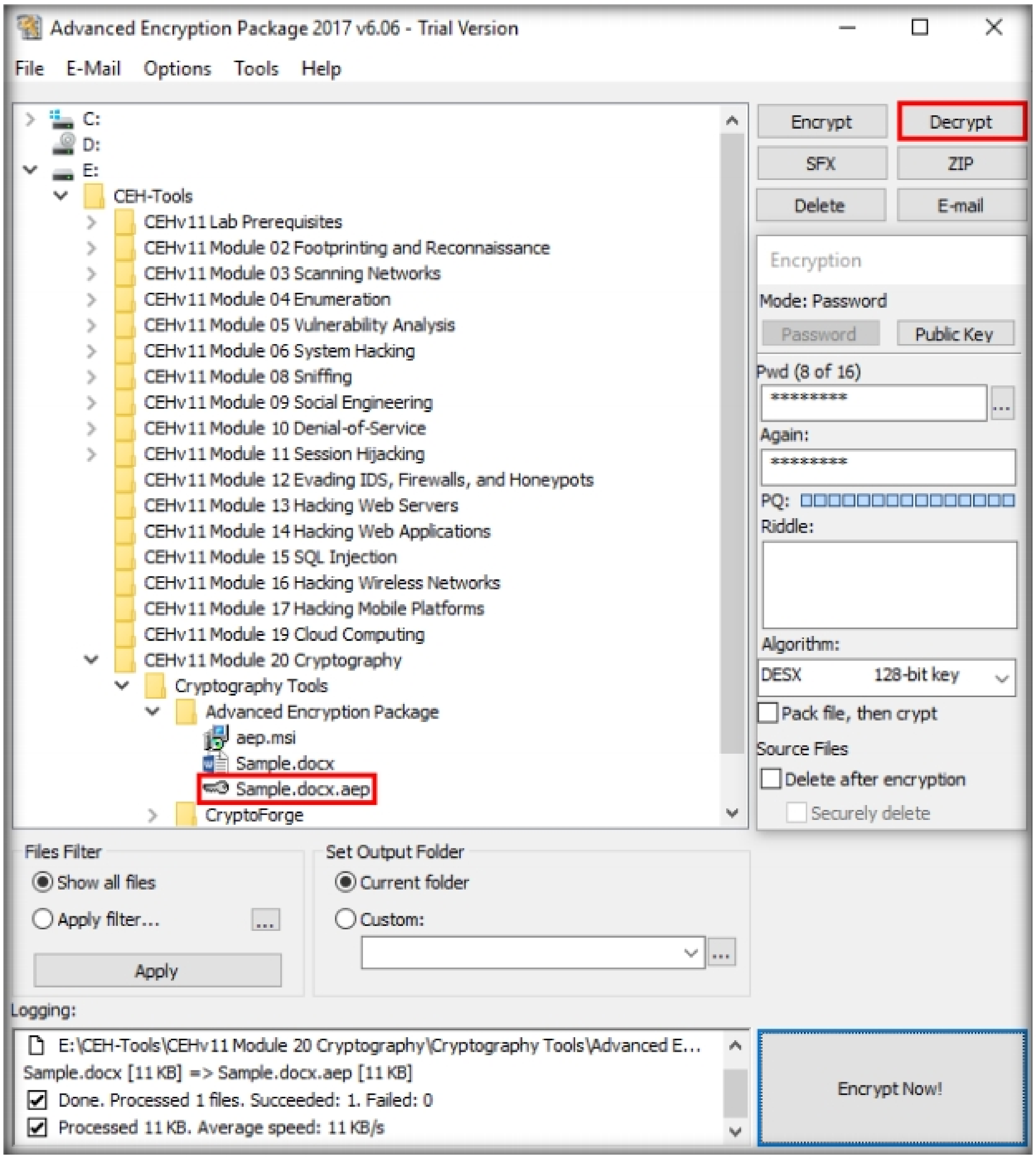
● Show all files ○ Apply filter...

● Current folder ○ Custom:

Figure 1.5.9: Encrypting the selected file

12. The encrypted **Sample.docx.aep** file appears in the same location as the original file (i.e., **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package**).

13. To decrypt the file, first, select the encrypted file and click on **Decrypt**.


Advanced Encryption Package 2017 v6.06 - Trial Version
File
E-Mail
Options
Tools
Help
C:
D:
E:
CEH-Tools
CEHv11 Lab Prerequisites
CEHv11 Module 02 Footprinting and Reconnaissance
CEHv11 Module 03 Scanning Networks
CEHv11 Module 04 Enumeration
CEHv11 Module 05 Vulnerability Analysis
CEHv11 Module 06 System Hacking
CEHv11 Module 08 Sniffing
CEHv11 Module 09 Social Engineering
CEHv11 Module 10 Denial-of-Service
CEHv11 Module 11 Session Hijacking
CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 15 SQL Injection
CEHv11 Module 16 Hacking Wireless Networks
CEHv11 Module 17 Hacking Mobile Platforms
CEHv11 Module 19 Cloud Computing
CEHv11 Module 20 Cryptography
Cryptography Tools
Advanced Encryption Package
aep.msi
Sample.docx
Sample.docx.aep
CryptoForge
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Encryption
Password
Public Key
PQ:
Riddle:
Pack file, then crypt
Source Files
Delete after encryption
Securely delete
Files Filter
Show all files
Apply filter...
Apply
Set Output Folder
Current folder
Custom:
Logging:
Encrypt Now!

Mode: Password

Pwd (8 of 16): *********

Again: *********

Algorithm: DESX 128-bit key

☐ Pack file, then crypt

☐ Delete after encryption

Files Filter: ● Show all files ○ Apply filter...

Set Output Folder: ● Current folder ○ Custom:

Logging:

```
E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced E...
Sample.docx [11 KB] => Sample.docx.aep [11 KB]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 11 KB. Average speed: 11 KB/s
```

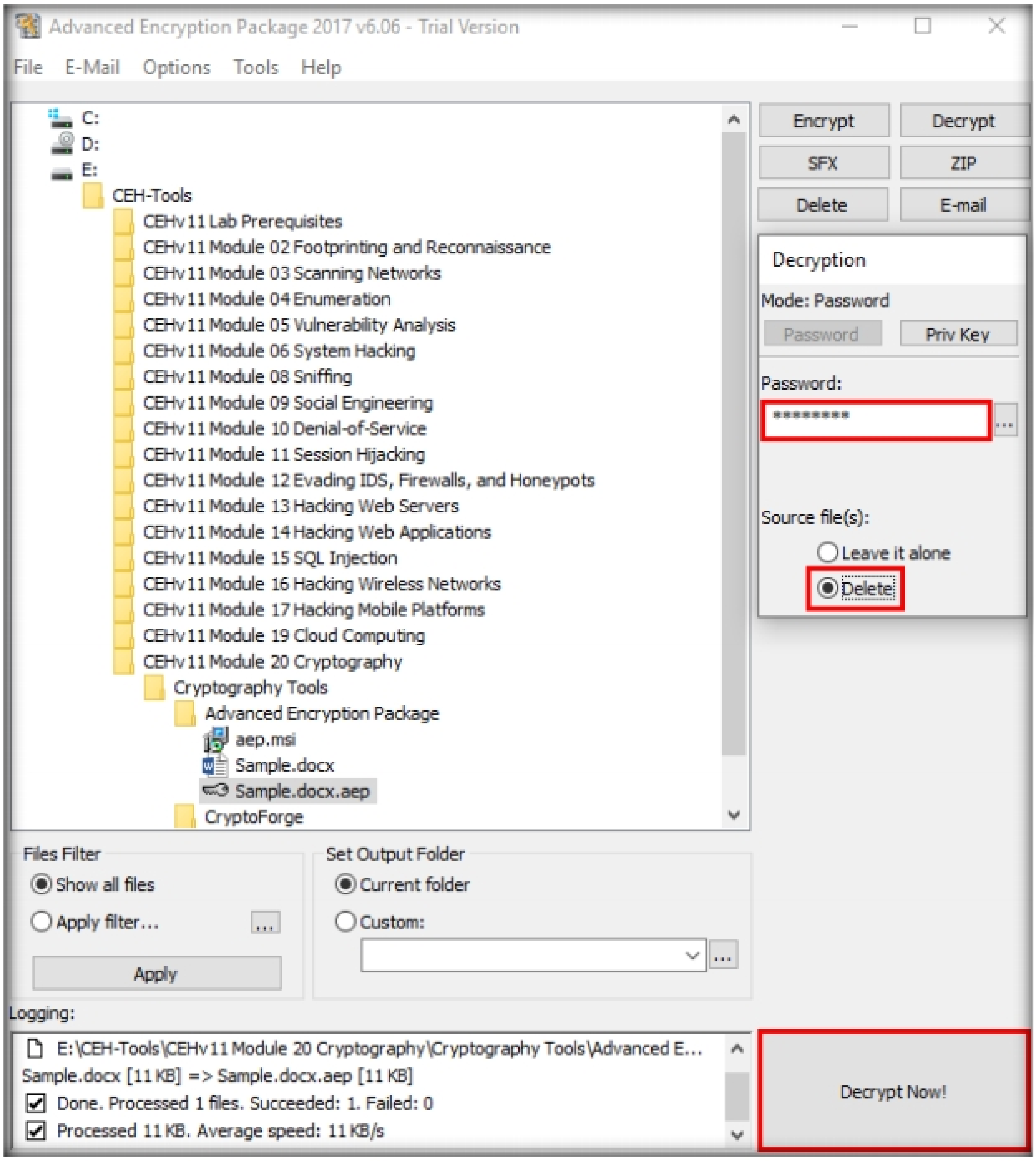
Figure 1.5.10: Decrypting the selected file

14. You will be prompted to enter the password. In the right-hand pane, under the **Password** field, enter the password that you have provided in **Step#11**.

TASK 5.3

Decrypt a File

15. Under the **Source file(s)** section in the right-pane, click the **Delete** radio-button to delete the source file **Sample.docx**; then, click **Decrypt Now!**.


Advanced Encryption Package 2017 v6.06 - Trial Version
File
E-Mail
Options
Tools
Help
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
C:
D:
E:
CEH-Tools
CEHv11 Lab Prerequisites
CEHv11 Module 02 Footprinting and Reconnaissance
CEHv11 Module 03 Scanning Networks
CEHv11 Module 04 Enumeration
CEHv11 Module 05 Vulnerability Analysis
CEHv11 Module 06 System Hacking
CEHv11 Module 08 Sniffing
CEHv11 Module 09 Social Engineering
CEHv11 Module 10 Denial-of-Service
CEHv11 Module 11 Session Hijacking
CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 15 SQL Injection
CEHv11 Module 16 Hacking Wireless Networks
CEHv11 Module 17 Hacking Mobile Platforms
CEHv11 Module 19 Cloud Computing
CEHv11 Module 20 Cryptography
Cryptography Tools
Advanced Encryption Package
aep.msi
Sample.docx
Sample.docx.aep
CryptoForge
Password
Priv Key
Apply
Decrypt Now!

Decryption

Mode: Password

Password: ********

Source file(s):
○ Leave it alone
● Delete

Files Filter
● Show all files
○ Apply filter...

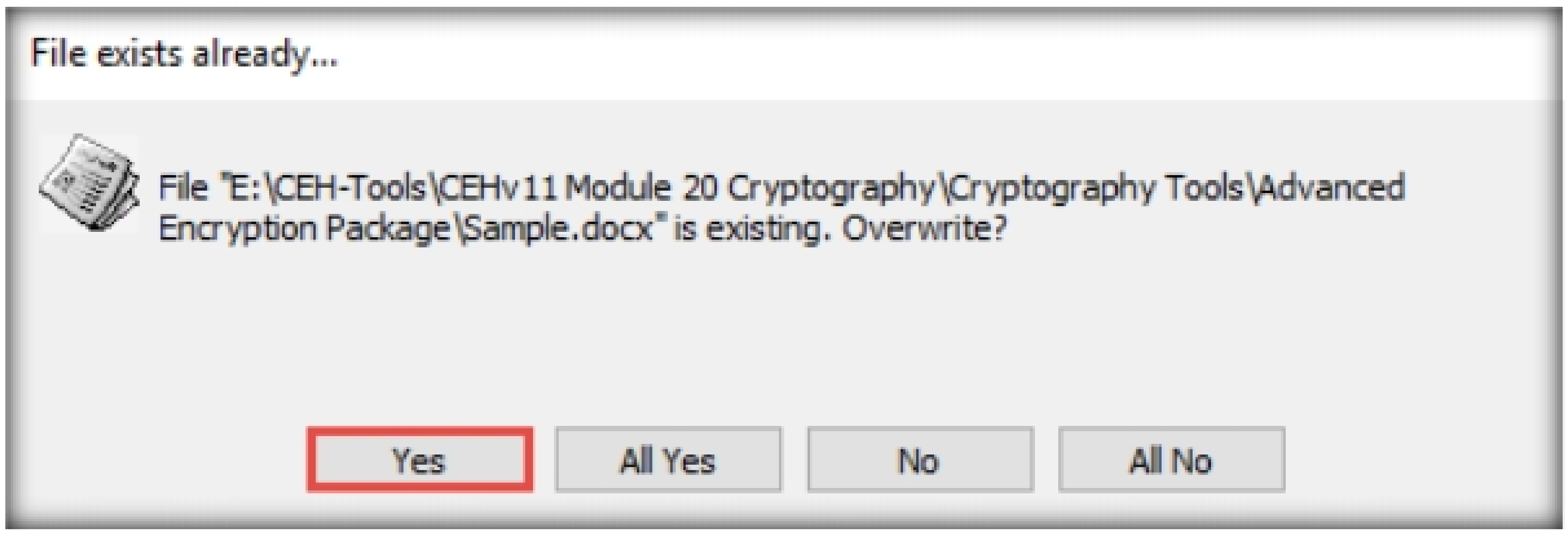
Set Output Folder
● Current folder
○ Custom:

Logging:

```
E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced E...
Sample.docx [11 KB] => Sample.docx.aep [11 KB]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 11 KB. Average speed: 11 KB/s
```

Figure 1.5.11: Decrypting the selected file

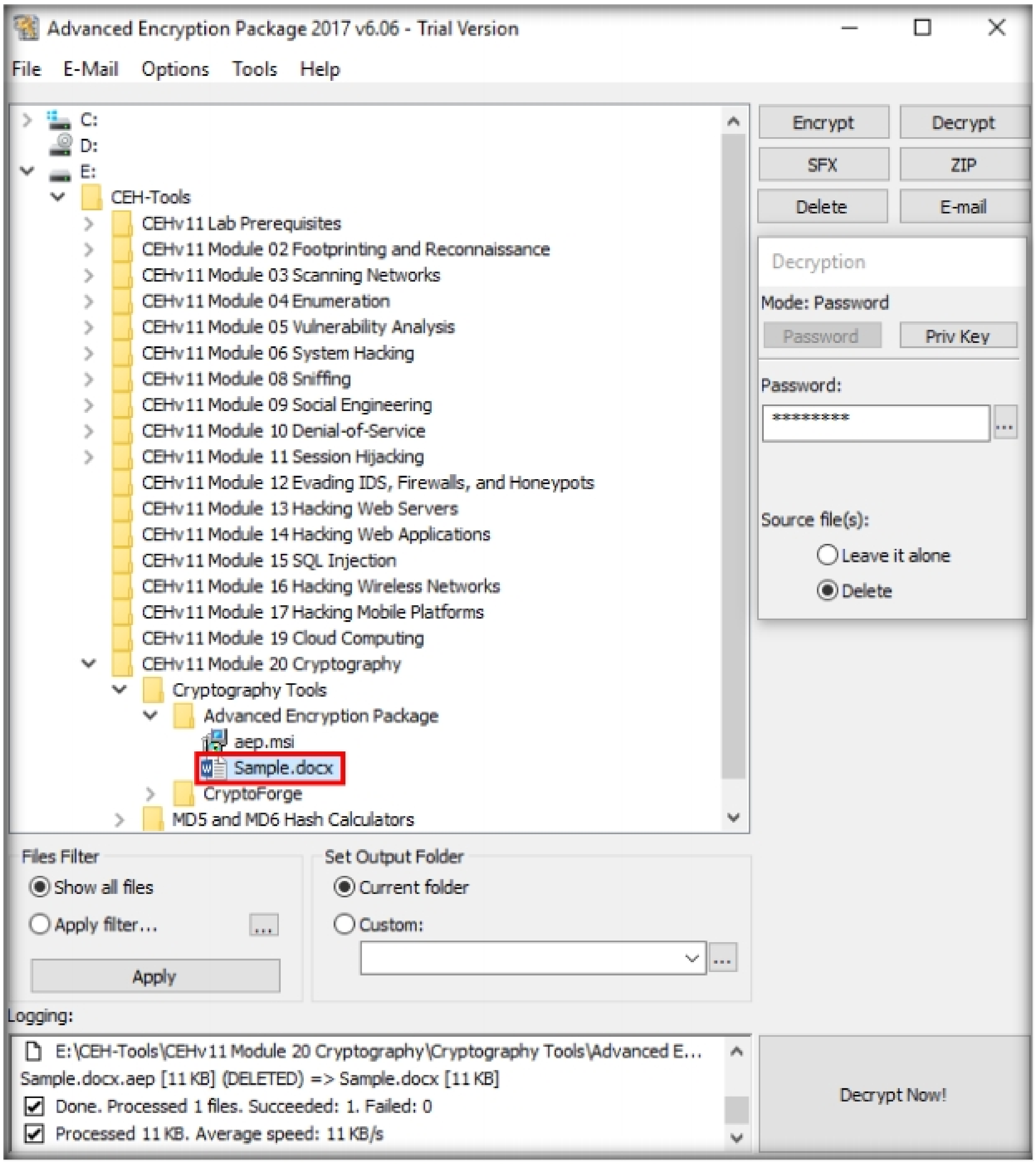
16. The **File exists already...** pop-up appears, click **Yes**.


File exists already...
Yes
All Yes
No
All No

File "E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced Encryption Package\Sample.docx" is existing. Overwrite?

Figure 1.5.12: File exists already… pop-up

17. The decrypted file (**Sample.docx**) appears in the same location, as shown in the screenshot.


Advanced Encryption Package 2017 v6.06 - Trial Version
File
E-Mail
Options
Tools
Help
C:
D:
E:
CEH-Tools
CEHv11 Lab Prerequisites
CEHv11 Module 02 Footprinting and Reconnaissance
CEHv11 Module 03 Scanning Networks
CEHv11 Module 04 Enumeration
CEHv11 Module 05 Vulnerability Analysis
CEHv11 Module 06 System Hacking
CEHv11 Module 08 Sniffing
CEHv11 Module 09 Social Engineering
CEHv11 Module 10 Denial-of-Service
CEHv11 Module 11 Session Hijacking
CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots
CEHv11 Module 13 Hacking Web Servers
CEHv11 Module 14 Hacking Web Applications
CEHv11 Module 15 SQL Injection
CEHv11 Module 16 Hacking Wireless Networks
CEHv11 Module 17 Hacking Mobile Platforms
CEHv11 Module 19 Cloud Computing
CEHv11 Module 20 Cryptography
Cryptography Tools
Advanced Encryption Package
aep.msi
Sample.docx
CryptoForge
MD5 and MD6 Hash Calculators
Encrypt
Decrypt
SFX
ZIP
Delete
E-mail
Decryption
Password
Priv Key
Files Filter
Apply
Set Output Folder
Logging:
Decrypt Now!

Mode: Password

Password: *********

Source file(s):
○ Leave it alone
● Delete

● Show all files
○ Apply filter…

● Current folder
○ Custom:

```
E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\Advanced E...
Sample.docx.aep [11 KB] (DELETED) => Sample.docx [11 KB]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 11 KB. Average speed: 11 KB/s
```

Figure 1.5.13: Decrypted file

Note: In real time, network administrators or ethical hackers use this tool to encrypt files and send it to the intended persons to safeguard the integrity of the files.

18. This concludes the demonstration of performing data encryption using the Advanced Encryption Package.

19. Close all open windows and document all the acquired information.

TASK 6

Encrypt and Decrypt Data using BCTextEncoder

Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

TASK 6.1

Encrypt the Data

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder_v.1.03.2.1.exe**.

2. The **BCTextEncoder Utility** window appears, as shown in the screenshot.

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

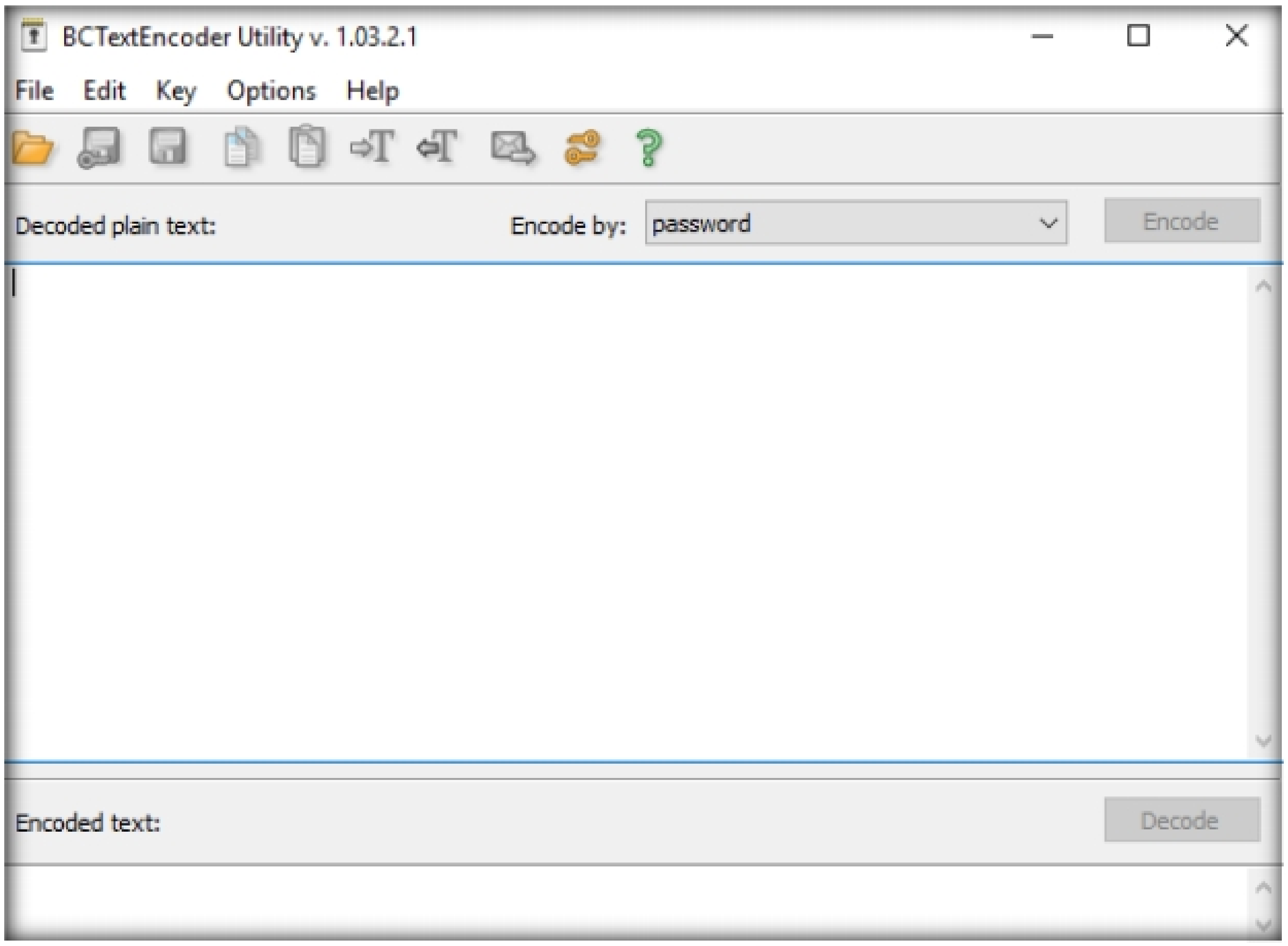


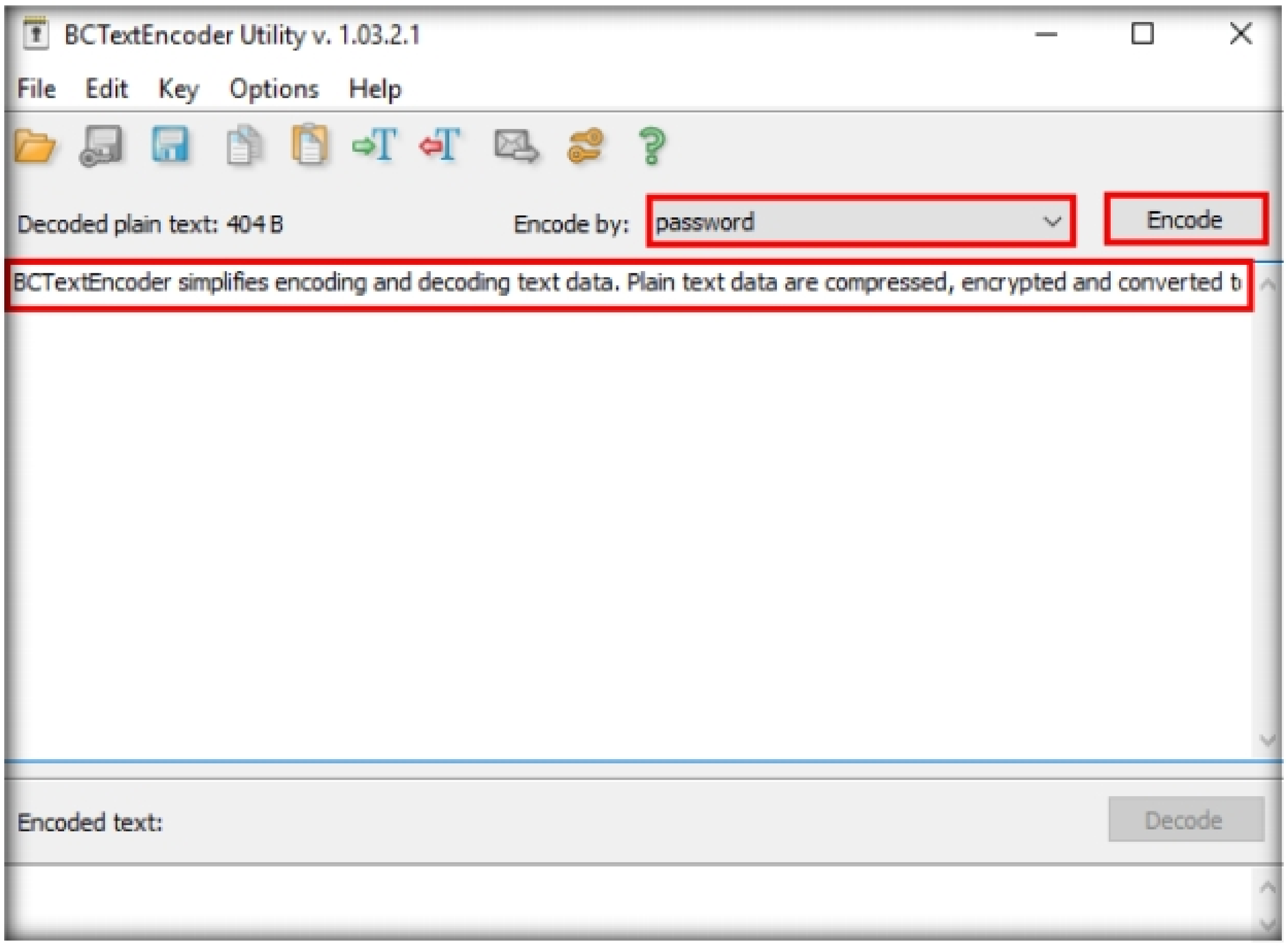
Figure 1.6.1: Main window of BCTextEncoder

3. To encrypt the text, insert text in the clipboard.

   Or

   Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

4. Ensure that the **password** option is selected in the **Encode by** field and click **Encode**.


BCTextEncoder Utility v. 1.03.2.1
File Edit Key Options Help
Decoded plain text: 404 B
Encode by: password
Encode
Encoded text:
Decode

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted t

Figure 1.6.2: BCTextEncoder: Secret information in clipboard

5. The **Enter password** pop-up appears; enter the password into the **Password** field and retype it in the **Confirm** field; then, click **OK**. Here, we use the password **test@123**.

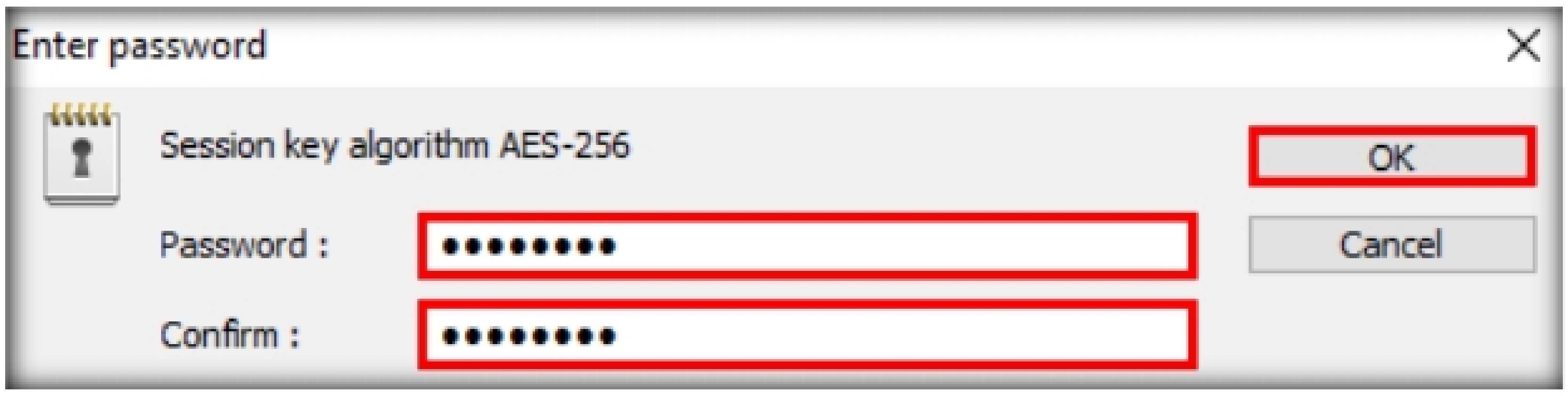
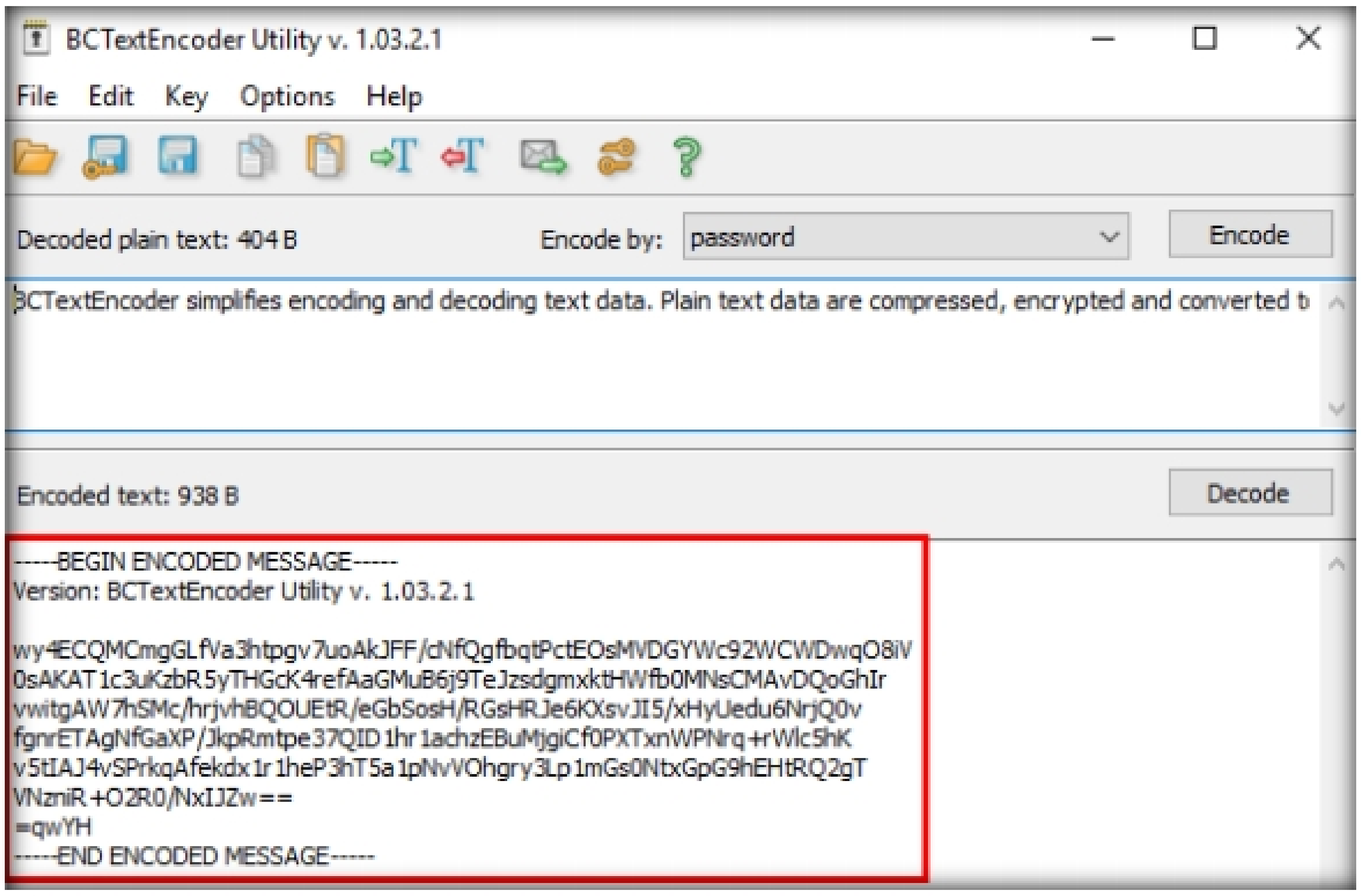

Enter password
Session key algorithm AES-256
Password : ••••••••
Confirm : ••••••••
OK
Cancel

Figure 1.6.3: Set the password for encryption

6. **BCTextEncoder** encodes the text and displays it in under the **Encoded text** section, as shown in the screenshot.


BCTextEncoder Utility v. 1.03.2.1
File
Edit
Key
Options
Help
Encode
Decode

Decoded plain text: 404 B

Encode by: password

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted t

Encoded text: 938 B

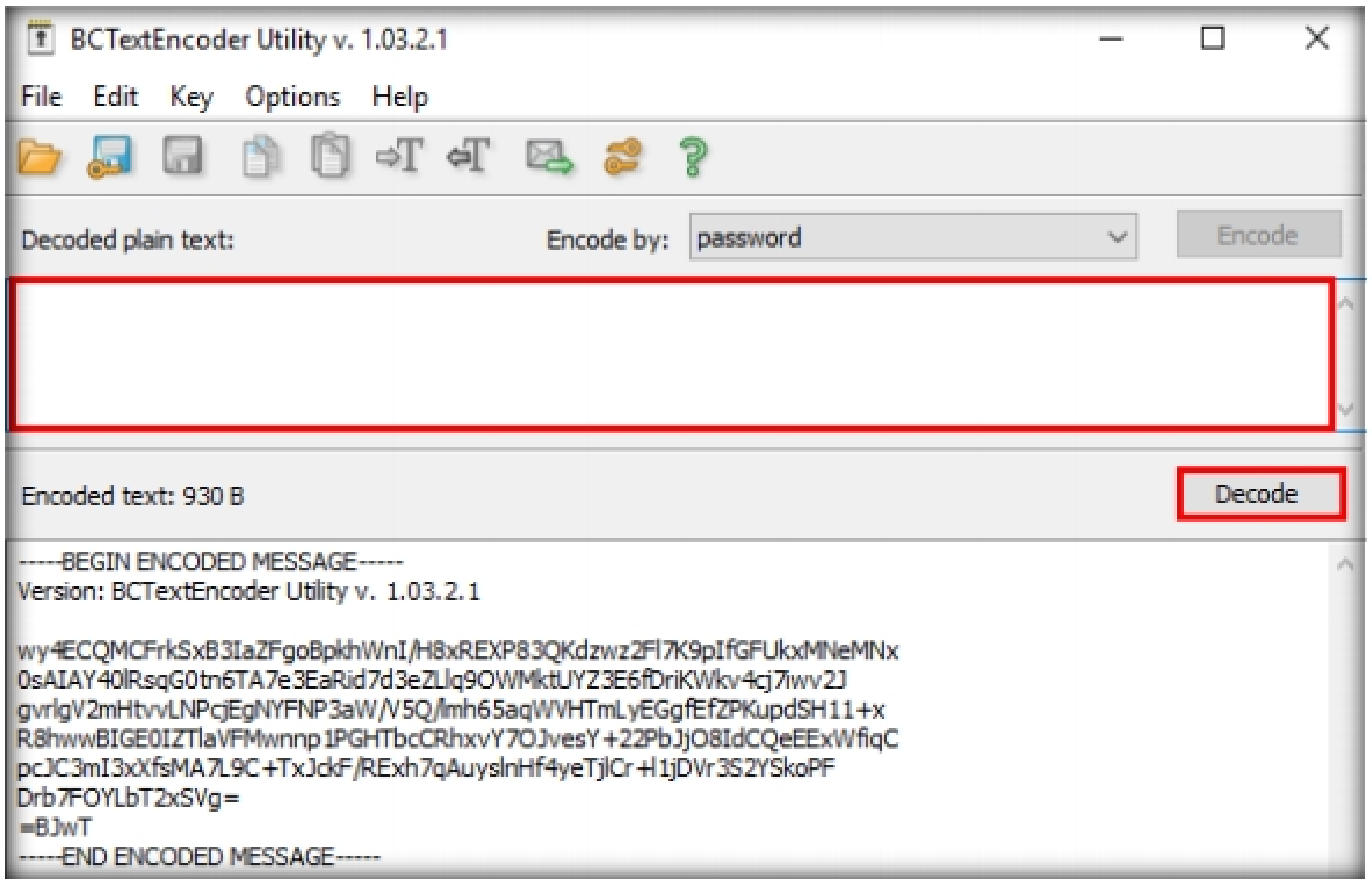
```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCmgGLfVa3htpgv7uoAkJFF/cNfQgfbqtPctEOsMVDGYWc92WCWDwqO8iV
0sAKAT1c3uKzbR5yTHGcK4refAaGMuB6j9TeJzsdgmxktHWfb0MNsCMAvDQoGhIr
vwitgAW7hSMc/hrjvhBQOUEtR/eGbSosH/RGsHRJe6KXsvJI5/xHyUedu6NrjQ0v
fgnrETAgNfGaXP/JkpRmtpe37QID1hr1achzEBuMjgiCf0PXTxnWPNrq+rWlc5hK
v5tIAJ4vSPrkqAfekdx1r1heP3hT5a1pNvVOhgry3Lp1mGs0NtxGpG9hEHtRQ2gT
VNzniR+O2R0/NxIJZw==
=qwYH
-----END ENCODED MESSAGE-----
```

Figure 1.6.4: Encoded text

TASK 6.2

Decrypt the Data

7. To decrypt the data, first, you need to clean the **Decoded plain text** in the clipboard, and then click the **Decode** button.


BCTextEncoder Utility v. 1.03.2.1
File
Edit
Key
Options
Help
Encode
Decode

Decoded plain text:

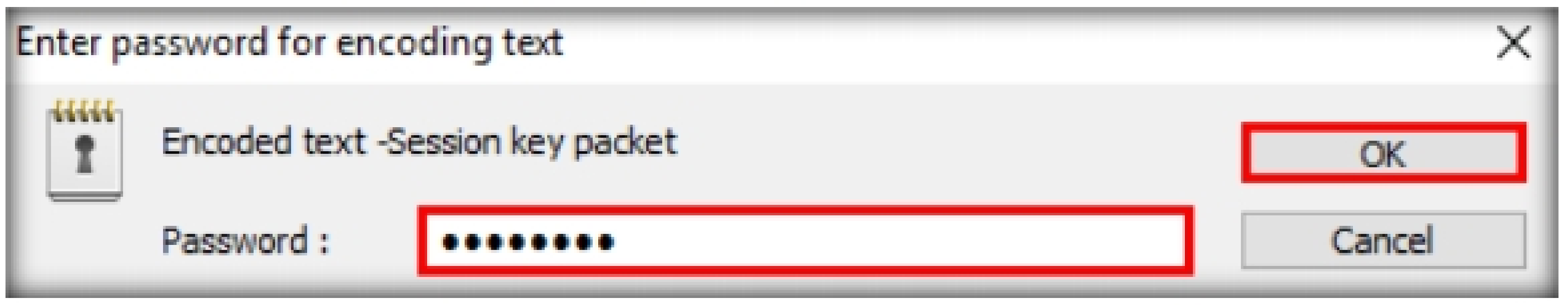
Encode by: password

Encoded text: 930 B

```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCFrkSxB3IaZFgoBpkhWnI/H8xREXP83QKdzwz2Fl7K9pIfGFUkxMNeMNx
0sAIAY40lRsqG0tn6TA7e3EaRid7d3eZLlq9OWMktUYZ3E6fDriKWkv4cj7iwv2J
gvrlgV2mHtvvLNPcjEgNYFNP3aW/V5Q/lmh65aqWVHTmLyEGgfEfZPKupdSH11+x
R8hwwBIGE0IZTlaVFMwnnp1PGHTbcCRhxvY7OJvesY+22PbJjO8IdCQeEExWfiqC
pcJC3mI3xXfsMA7L9C+TxJckF/RExh7qAuyslnHf4yeTjlCr+l1jDVr3S2YSkoPF
Drb7FOYLbT2xSVg=
=BJwT
-----END ENCODED MESSAGE-----
```

Figure 1.6.5: Decoding data

8. The **Enter password for encoding text** dialog-box appears; insert the **Password** (**test@123**) into the password field and click **OK**.


Enter password for encoding text
OK
Cancel

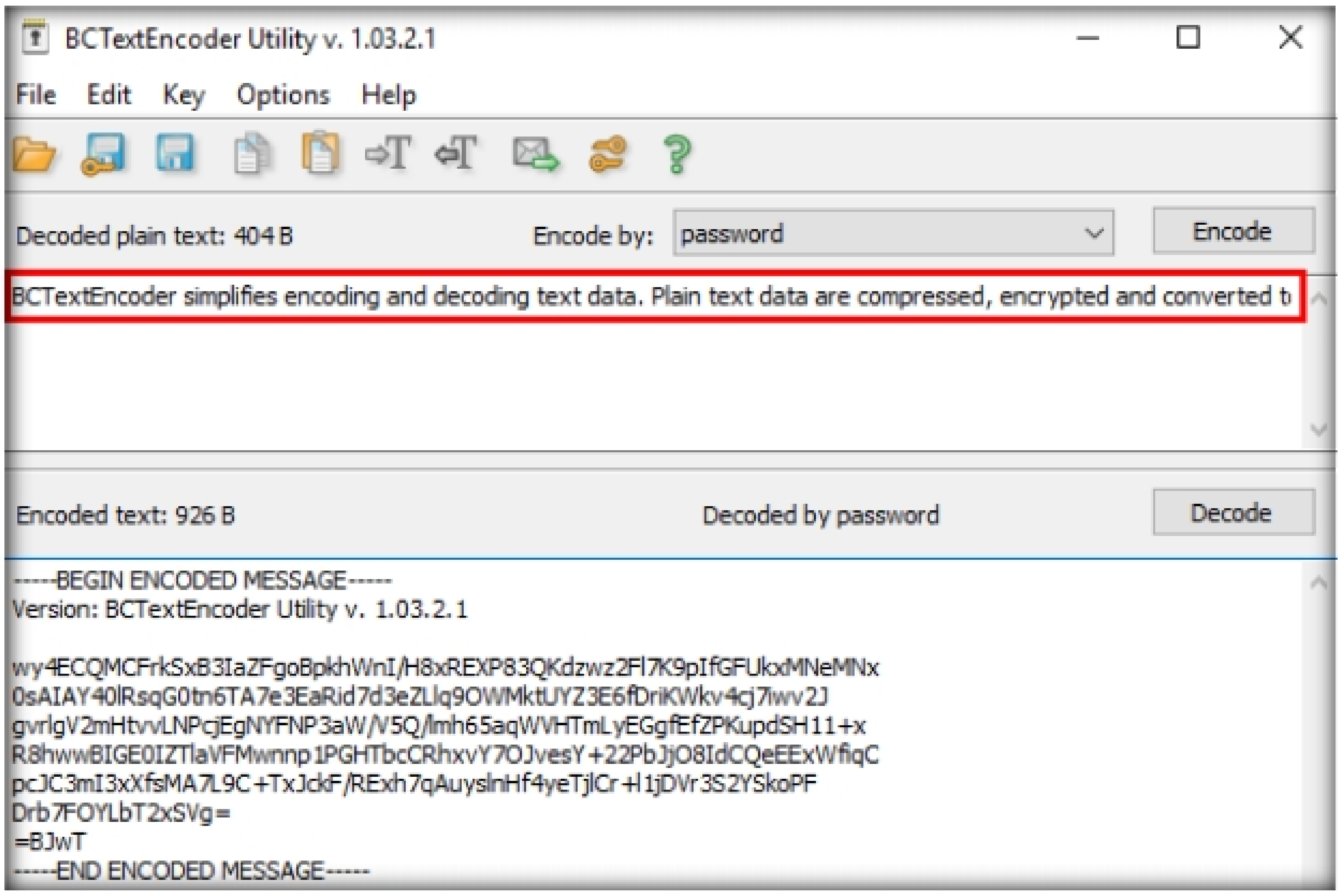
Encoded text -Session key packet

Password : ••••••••

Figure 1.6.6: Enter the password for decoding

You can also use other cryptography tools such as **AxCrypt** (https://www.axcrypt.net), **Microsoft Cryptography Tools** (https://docs.microsoft.com), and **Concealer** (https://www.belightsoft.com) to encrypt confidential data.

9. The decoded plain text appears under the **Decoded plain text** section, as shown in the screenshot.



Decoded plain text: 404 B

Encode by: password

BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted and converted t

Encoded text: 926 B

Decoded by password

```
-----BEGIN ENCODED MESSAGE-----
Version: BCTextEncoder Utility v. 1.03.2.1

wy4ECQMCFrkSxB3IaZFgoBpkhWnI/H8xREXP83QKdzwz2Fl7K9pIfGFUkxMNeMNx
0sAIAY40lRsqG0tn6TA7e3EaRid7d3eZLlq9OWMktUYZ3E6fDriKWkv4cj7iwv2J
gvrlgV2mHtvvLNPcjEgNYFNP3aW/V5Q/lmh65aqWVHTmLyEGgfEfZPKupdSH11+x
R8hwwBIGE0IZTlaVFMwnnp1PGHTbcCRhxvY7OJvesY+22PbJjO8IdCQeEExWfiqC
pcJC3mI3xXfsMA7L9C+TxJckF/RExh7qAuyslnHf4yeTjlCr+l1jDVr3S2YSkoPF
Drb7FOYLbT2xSVg=
=BJwT
-----END ENCODED MESSAGE-----
```

Figure 1.6.7: Output decoded text

Note: In real-time, using this procedure, you can encode the text while sending it to the intended user along with the password used for encryption. The user for whom the text is intended should have the BCTextEncoder application installed on his/her machine. He/she will have to paste the encoded text into the **Encoded text** section and use the password you shared, to decode it to plain text.

10. This concludes the demonstration of encrypting and decrypting the data using BCTextEncoder.

11. Close all open windows and document all the acquired information.

12. Turn off the **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 2

Create a Self-signed Certificate

A self-signed certificate is an identity certificate signed by the same entity whose identity it verifies.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned.

The labs in this exercise demonstrate the creation of a self-signed certificate.

Lab Objectives

- Create and use self-signed certificates

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Duration

Time: 10 Minutes

Overview of Self-signed Certificate

In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

Lab Tasks

TASK 1

Create and Use Self-signed Certificates

Here, we will create a self-signed certificate in Windows Server 2019.

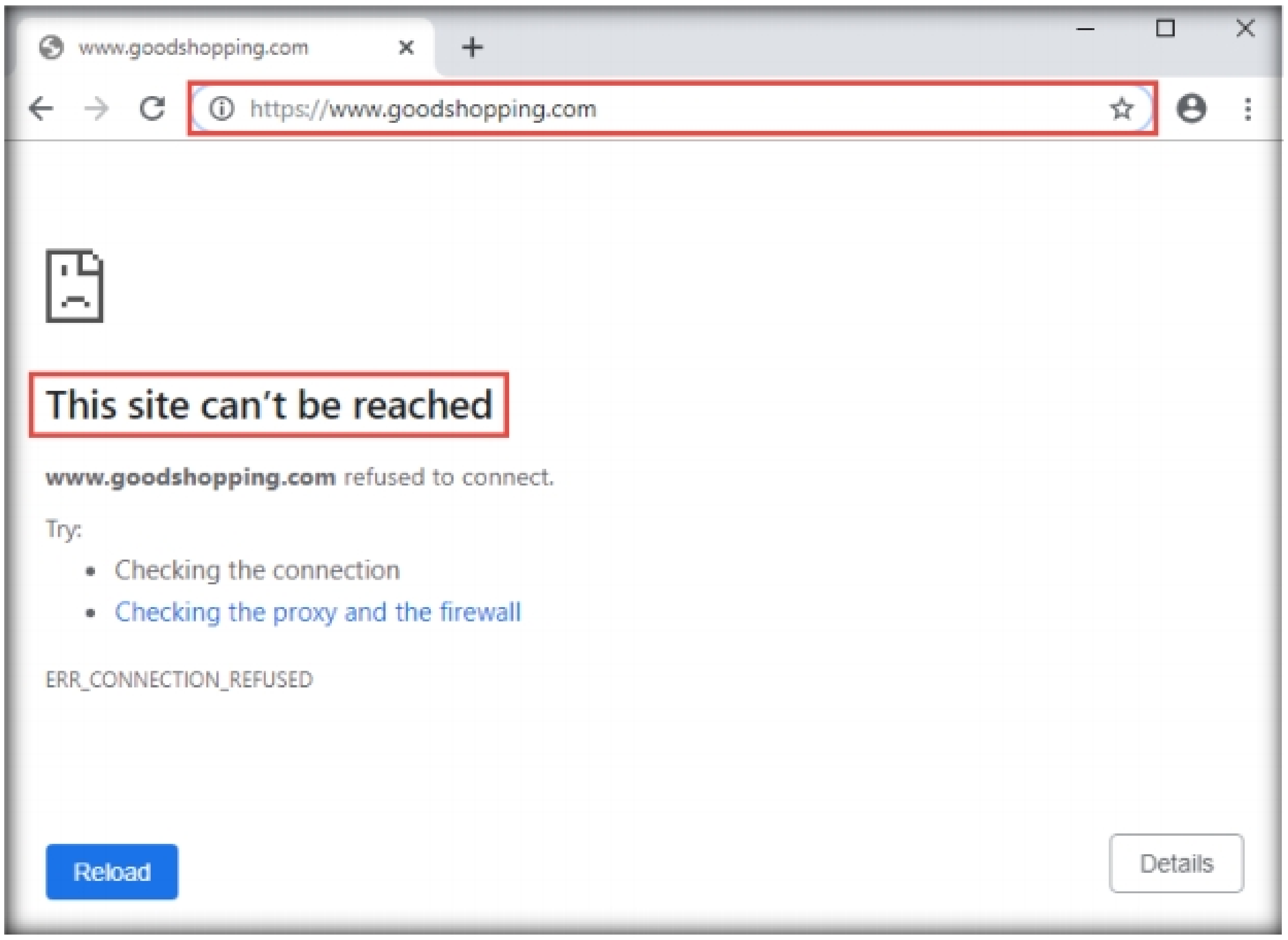
1. Turn on the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.1

Verify Self-Signed Certificate

2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser (here, **Google Chrome**), type **https://www.goodshopping.com** in the address bar, and press **Enter**.
4. As you are using an https channel to browse the website, it displays a page stating that **This site can't be reached**.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Close the web browser.

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key.



This site can't be reached

www.goodshopping.com refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

Figure 2.1.1: www.goodshopping.com before adding Certificate

TASK 1.2

Launch IIS Manager

6. Click the **Type here to search** icon ( ) present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.

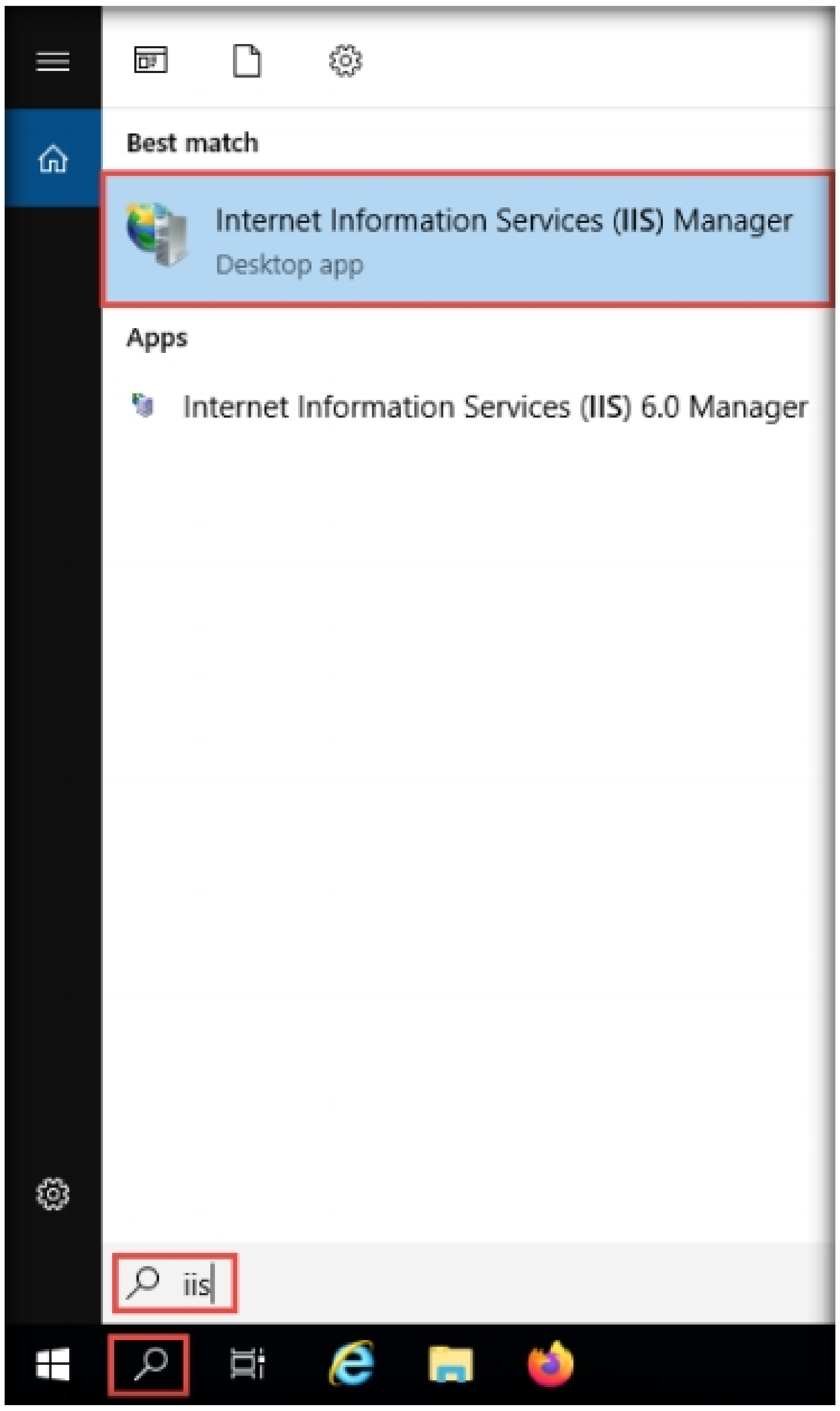

Best match
Internet Information Services (IIS) Manager
Desktop app
Apps
Internet Information Services (IIS) 6.0 Manager
iis

Figure 2.1.2: Launch IIS Manager

The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

TASK 1.3

Configure Server Certificates

7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator)**) under the **Connections** section from the left-hand pane.

8. In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.

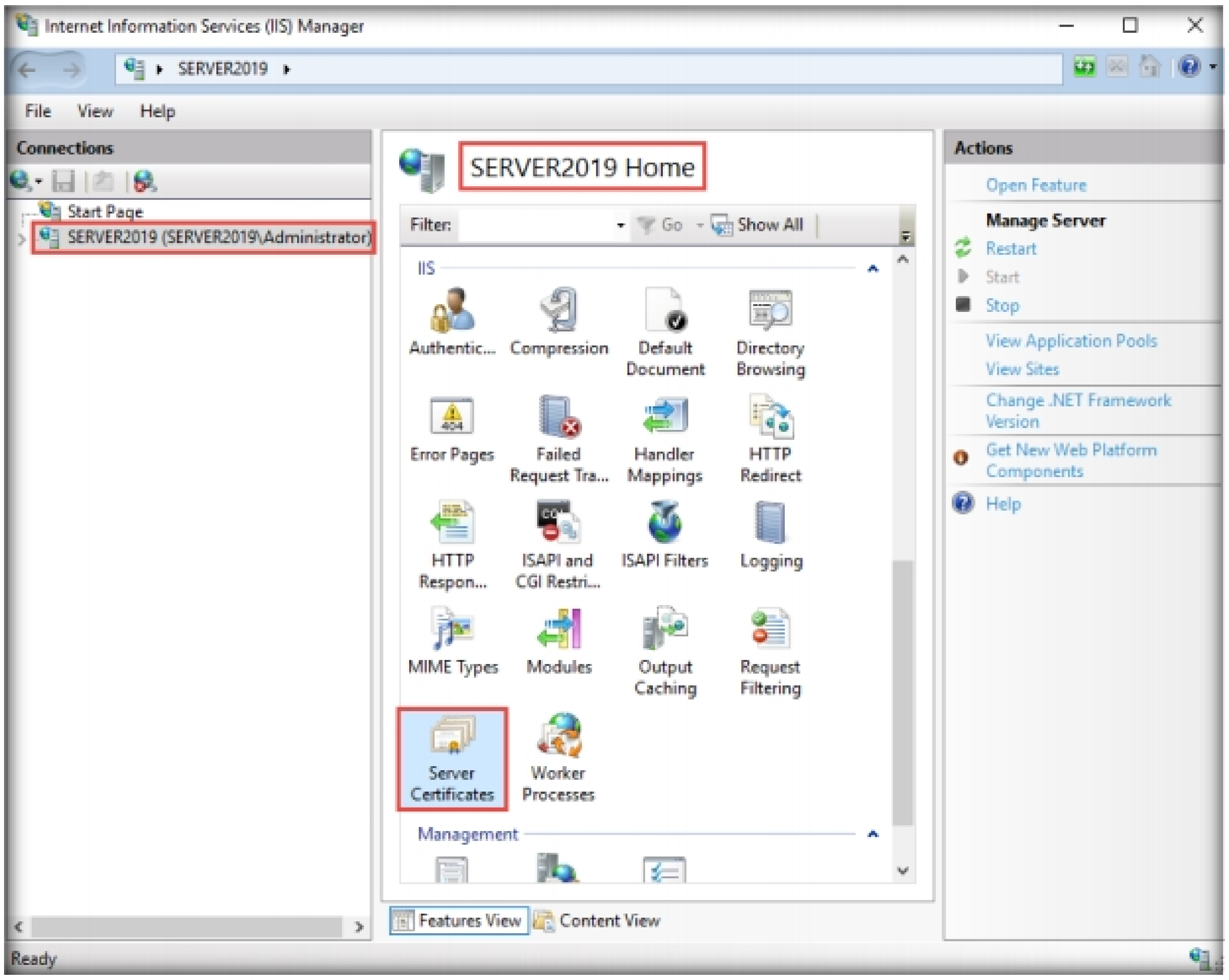
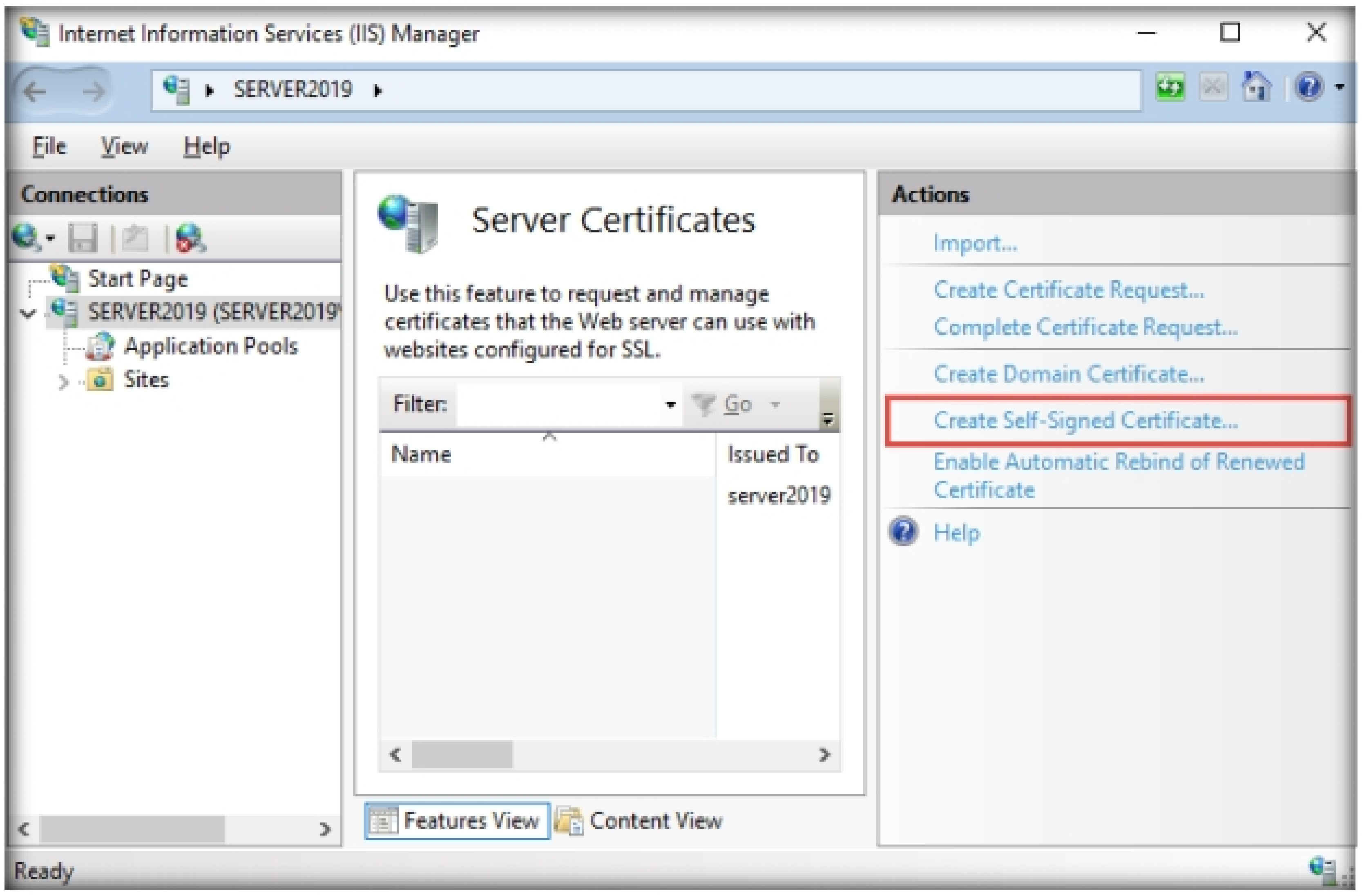

Internet Information Services (IIS) Manager
SERVER2019
File View Help
Connections
Start Page
SERVER2019 (SERVER2019\Administrator)
SERVER2019 Home
Filter:
Go
Show All
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Failed Request Tra...
Handler Mappings
HTTP Redirect
HTTP Respon...
ISAPI and CGI Restri...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
Server Certificates
Worker Processes
Management
Features View
Content View
Actions
Open Feature
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Change .NET Framework Version
Get New Web Platform Components
Help
Ready

Figure 2.1.3: IIS Manager Server Certificates

TASK 1.4

Create a Self-signed Certificate

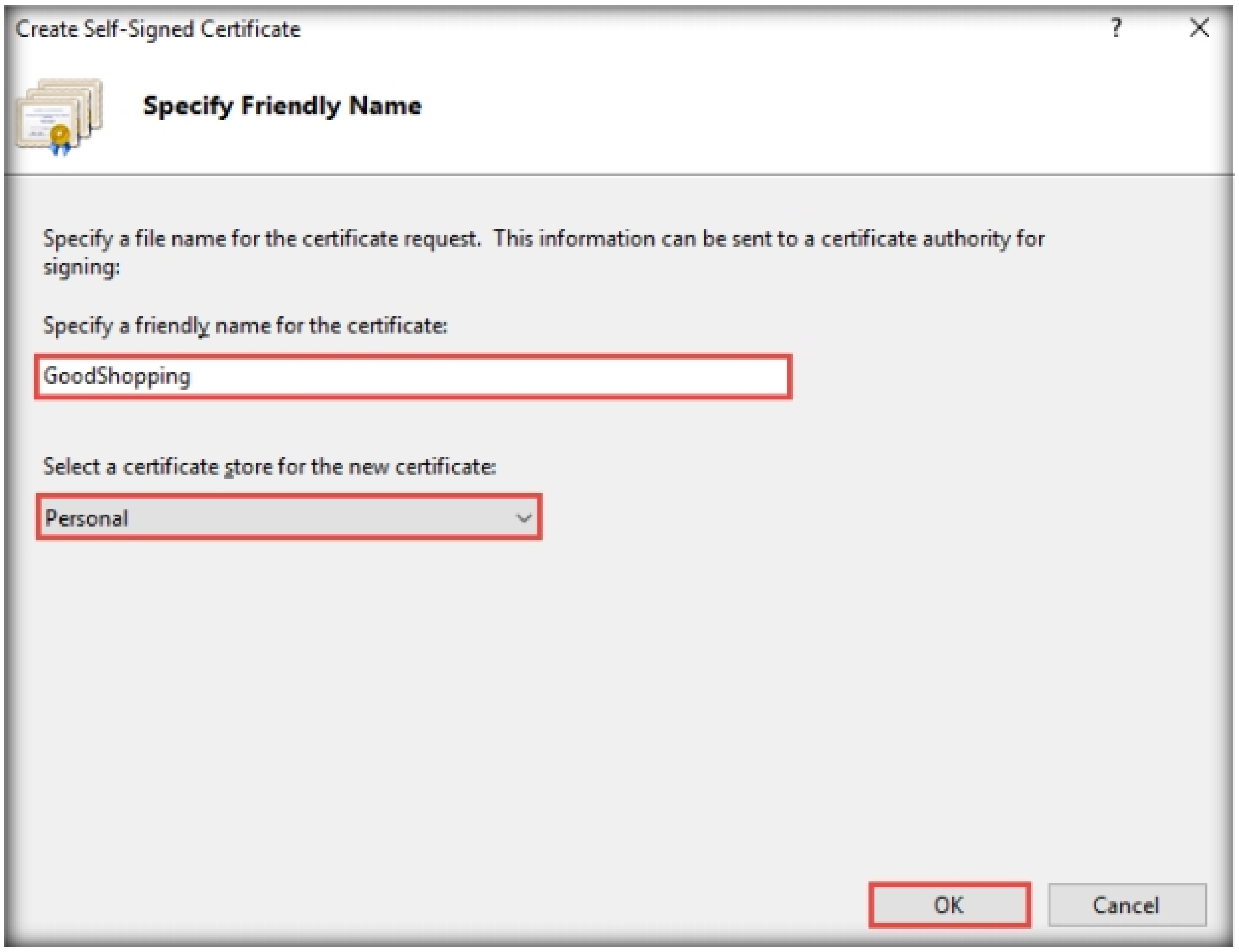
9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.


Internet Information Services (IIS) Manager
SERVER2019
File View Help
Connections
Start Page
SERVER2019 (SERVER2019
Application Pools
Sites
Server Certificates
Filter:
Go
Name
Issued To
server2019
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Figure 2.1.4: Server Certificates

10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.


Create Self-Signed Certificate
?
Specify Friendly Name
OK
Cancel

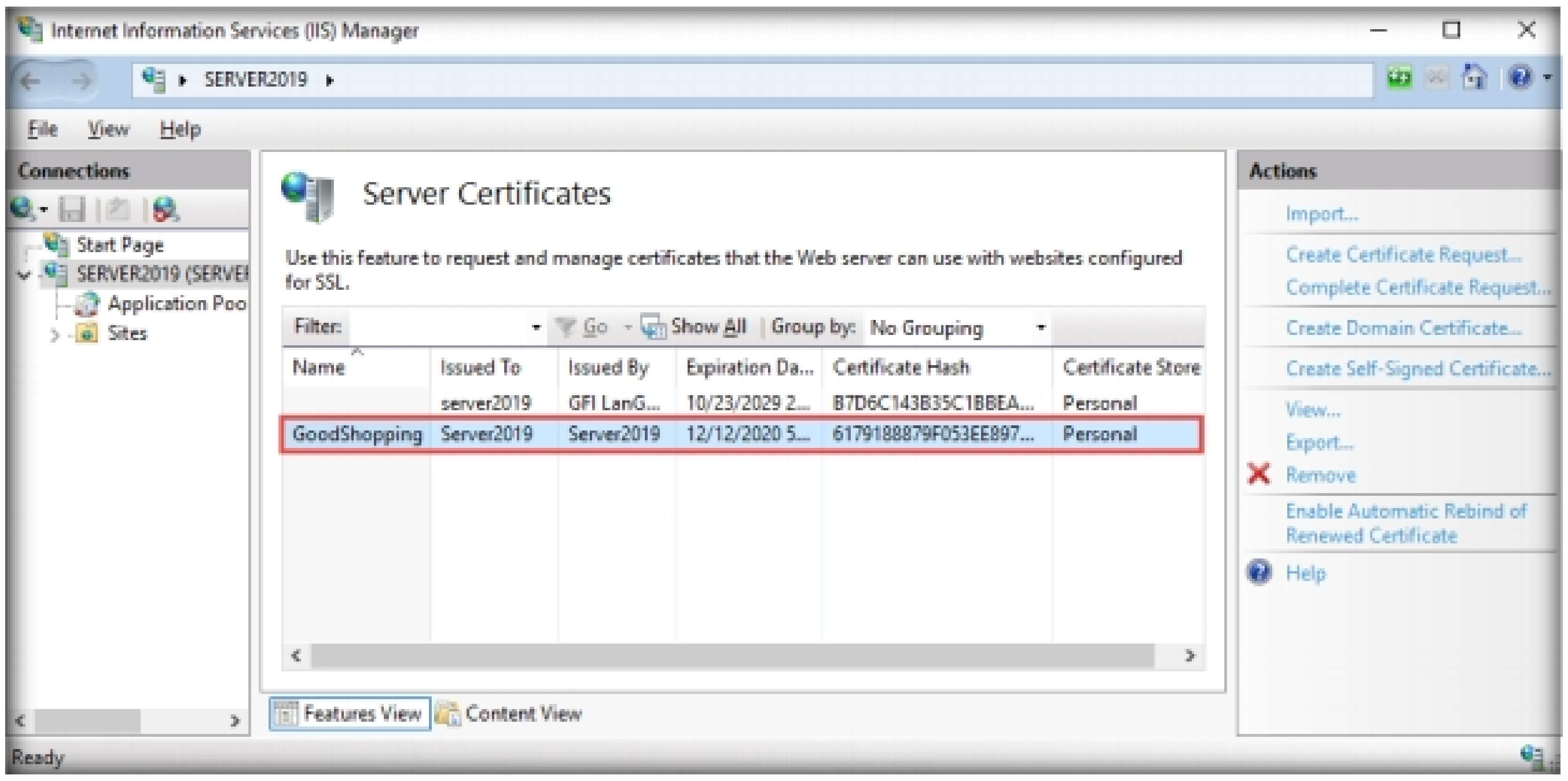
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate: GoodShopping

Select a certificate store for the new certificate: Personal

Figure 2.1.5: Specify Friendly Name

11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.


Internet Information Services (IIS) Manager
SERVER2019
File
View
Help
Connections
Start Page
SERVER2019 (SERVEI
Application Poo
Sites
Server Certificates
Filter:
Go
Show All
Group by:
No Grouping
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Da...	Certificate Hash	Certificate Store
	server2019	GFI LanG...	10/23/2029 2...	B7D6C143B35C1BBEA...	Personal
GoodShopping	Server2019	Server2019	12/12/2020 5...	6179188879F053EE897...	Personal

Figure 2.1.6: Server Certificates

TASK 1.5

Edit Bindings

12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings...** from the right-hand pane in the **Actions** section.

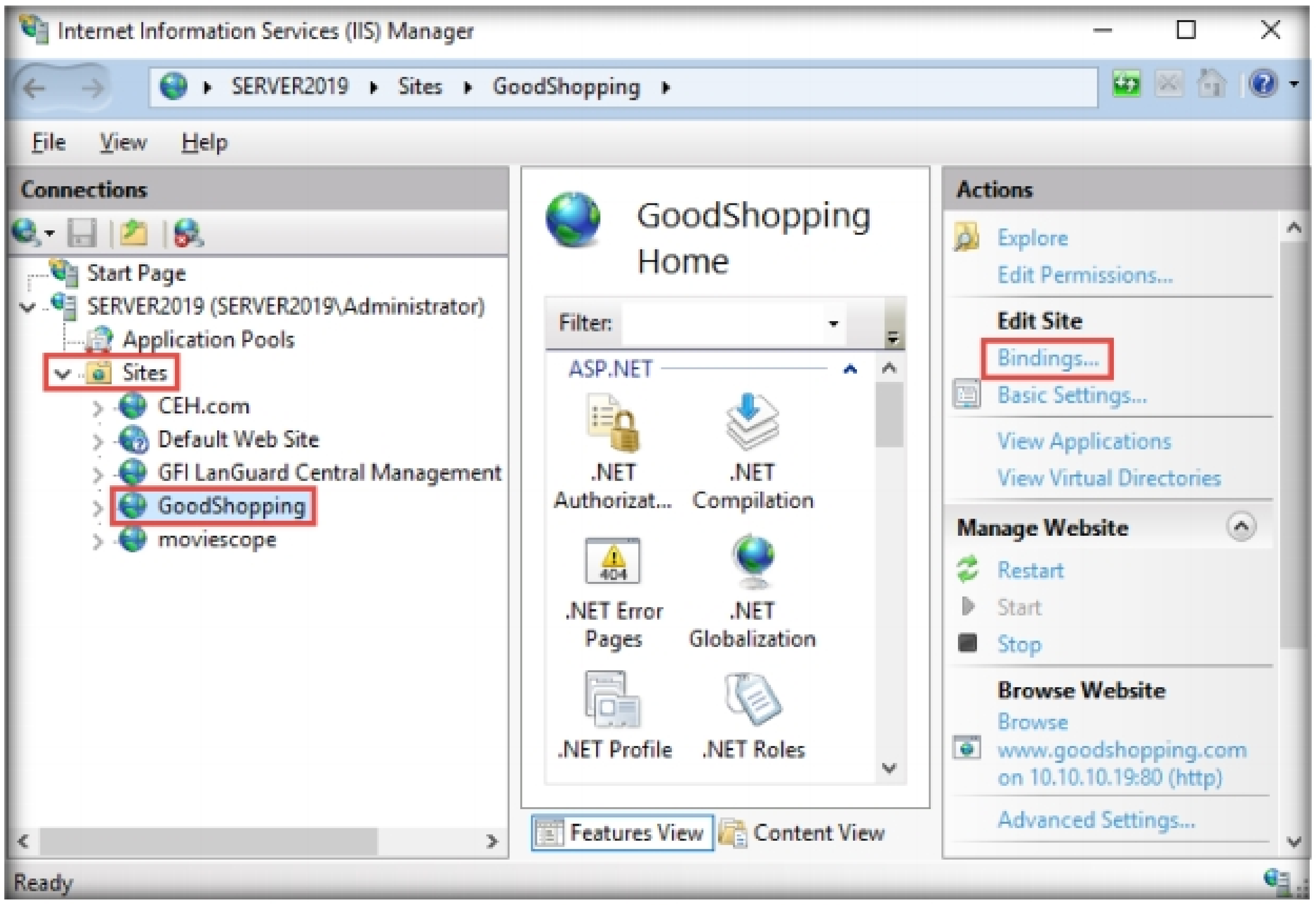
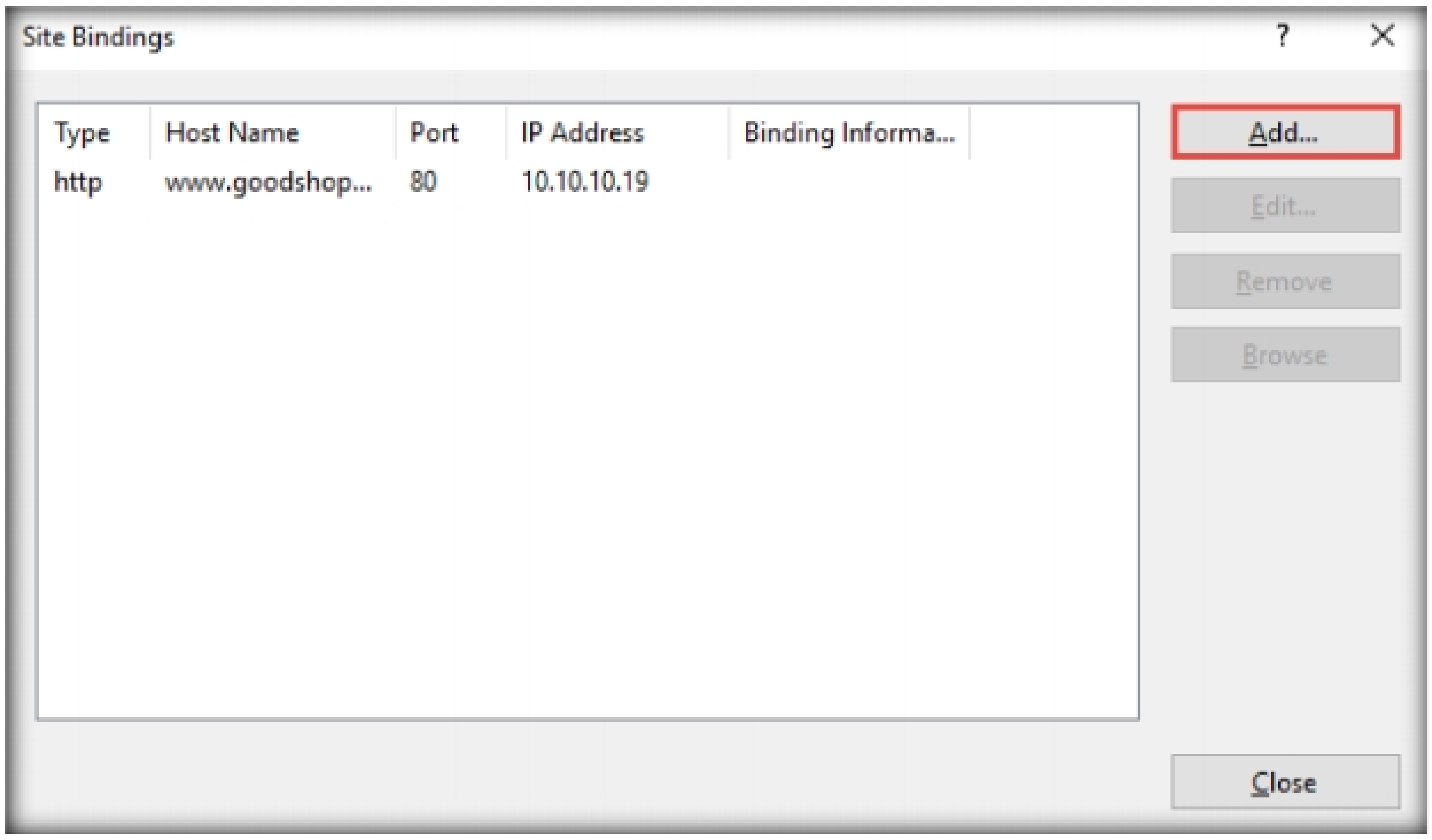

Internet Information Services (IIS) Manager
SERVER2019 ▸ Sites ▸ GoodShopping ▸
File View Help
Connections
Start Page
SERVER2019 (SERVER2019\Administrator)
Application Pools
Sites
CEH.com
Default Web Site
GFI LanGuard Central Management
GoodShopping
moviescope
GoodShopping Home
Filter:
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
Features View
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse www.goodshopping.com on 10.10.10.19:80 (http)
Advanced Settings...
Ready

Figure 2.1.7: Editing Site Bindings

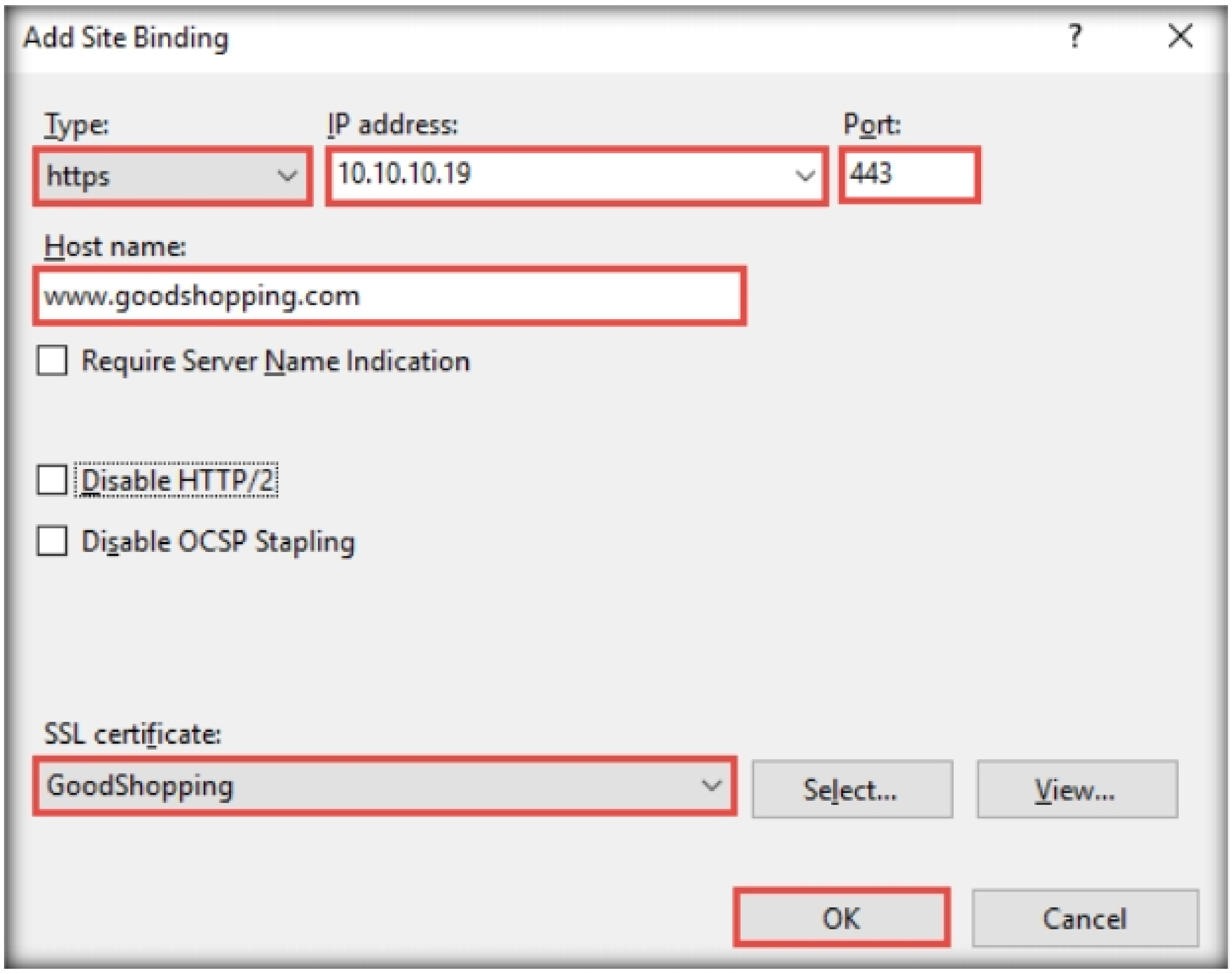
13. The **Site Bindings** window appears; click **Add...**.


Site Bindings
Add...
Edit...
Remove
Browse
Close

Type	Host Name	Port	IP Address	Binding Informa...
http	www.goodshop...	80	10.10.10.19	

Figure 2.1.8: Site Bindings window

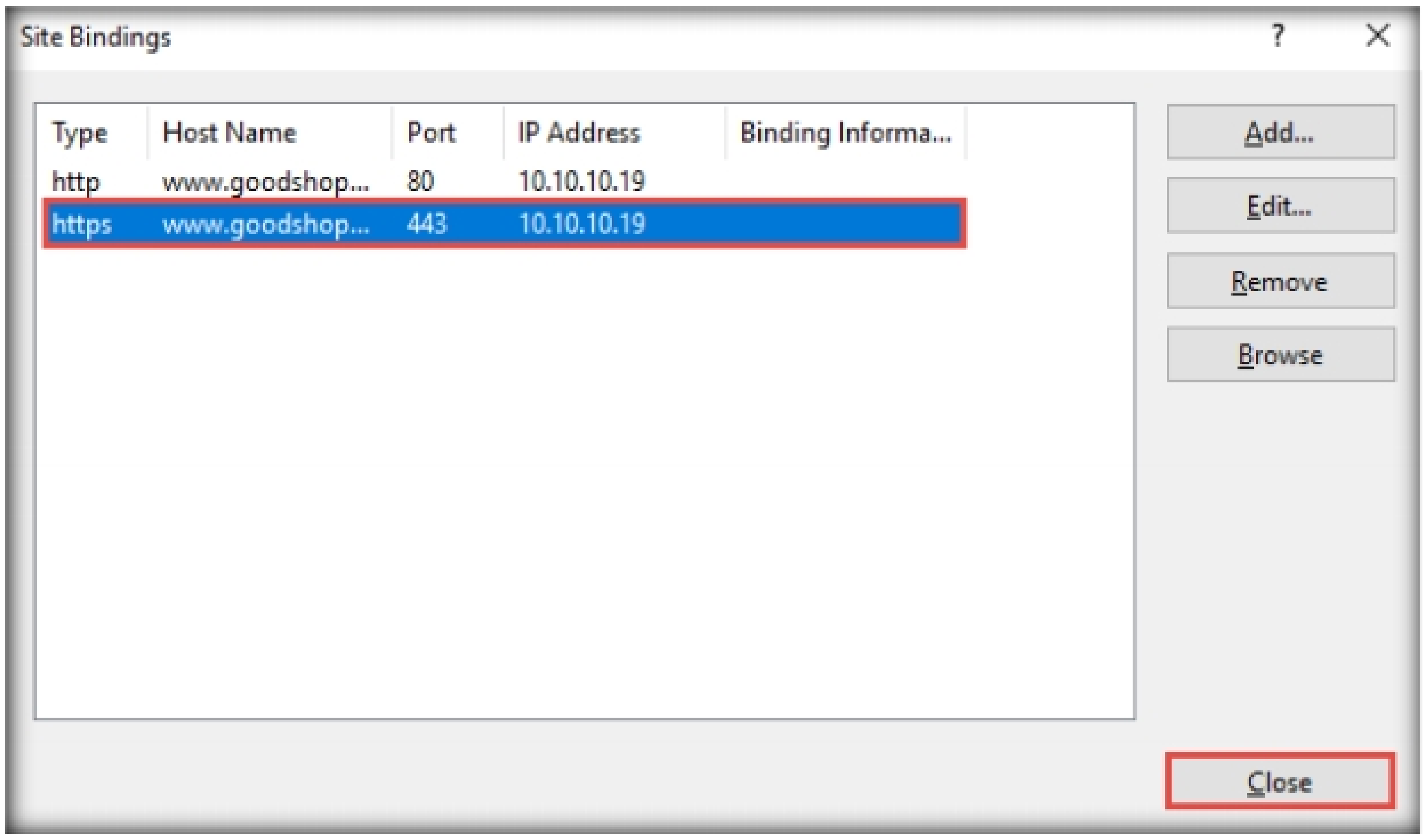
14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).
15. Choose the **IP address** on which the site is hosted (here, **10.10.10.19**).
16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.



Type: https
IP address: 10.10.10.19
Port: 443
Host name: www.goodshopping.com
☐ Require Server Name Indication
☐ Disable HTTP/2
☐ Disable OCSP Stapling
SSL certificate: GoodShopping

Figure 2.1.9: Adding Site Binding

17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.

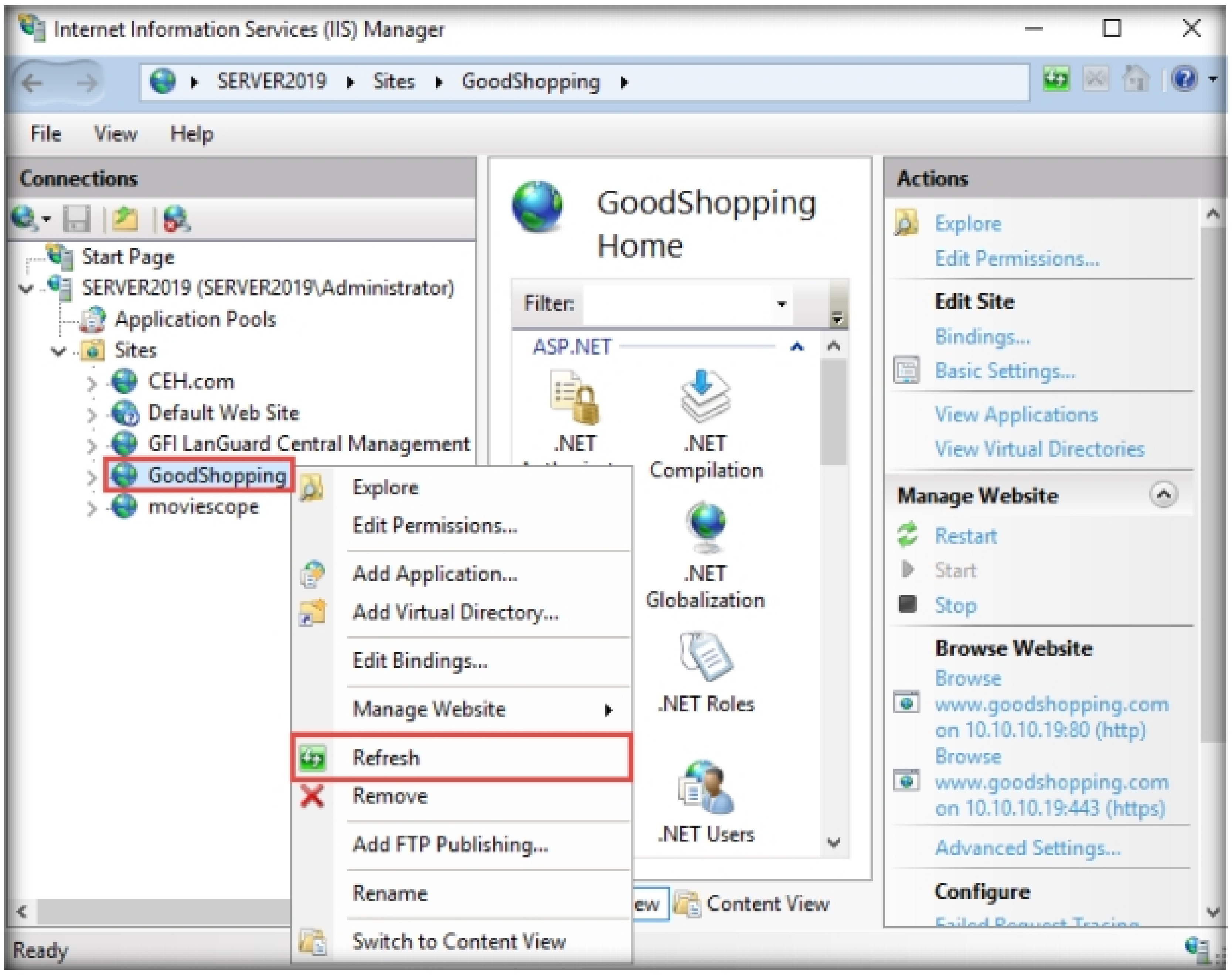


Site Bindings
?
Add...
Edit...
Remove
Browse
Close

Type	Host Name	Port	IP Address	Binding Informa...
http	www.goodshop...	80	10.10.10.19	
https	www.goodshop...	443	10.10.10.19	

Figure 2.1.10: Added HTTPS Channel

18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.



Internet Information Services (IIS) Manager
SERVER2019 ▸ Sites ▸ GoodShopping ▸
File View Help
Connections
Start Page
SERVER2019 (SERVER2019\Administrator)
Application Pools
Sites
CEH.com
Default Web Site
GFI LanGuard Central Management
GoodShopping
moviescope
Explore
Edit Permissions...
Add Application...
Add Virtual Directory...
Edit Bindings...
Manage Website
Refresh
Remove
Add FTP Publishing...
Rename
Switch to Content View
GoodShopping Home
Filter:
ASP.NET
.NET Authorization
.NET Compilation
.NET Globalization
.NET Roles
.NET Users
Content View
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse www.goodshopping.com on 10.10.10.19:80 (http)
Browse www.goodshopping.com on 10.10.10.19:443 (https)
Advanced Settings...
Configure
Failed Request Tracing...
Ready

Figure 2.1.11: Added HTTPS Channel

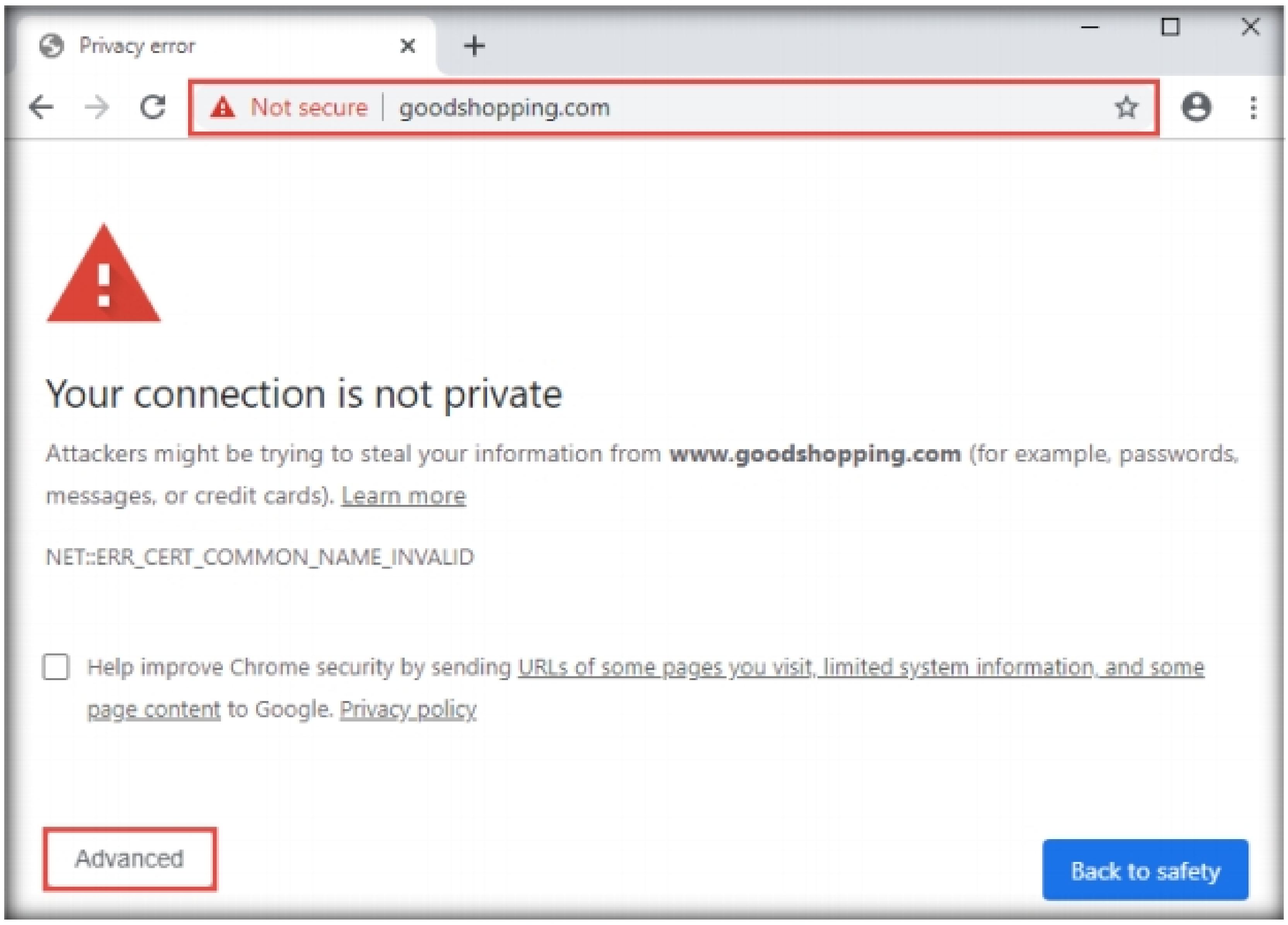
19. Minimize the **Internet Information Services (IIS) Manager** window.

TASK 1.6

Open SSL Website

20. Open the **Google Chrome** browser, type **https://www.goodshopping.com** in the address bar, and press **Enter**.

21. The **Your connection is not private** message appears, click **ADVANCED** to proceed.


Privacy error
Not secure
goodshopping.com

Your connection is not private

Attackers might be trying to steal your information from **www.goodshopping.com** (for example, passwords, messages, or credit cards). Learn more

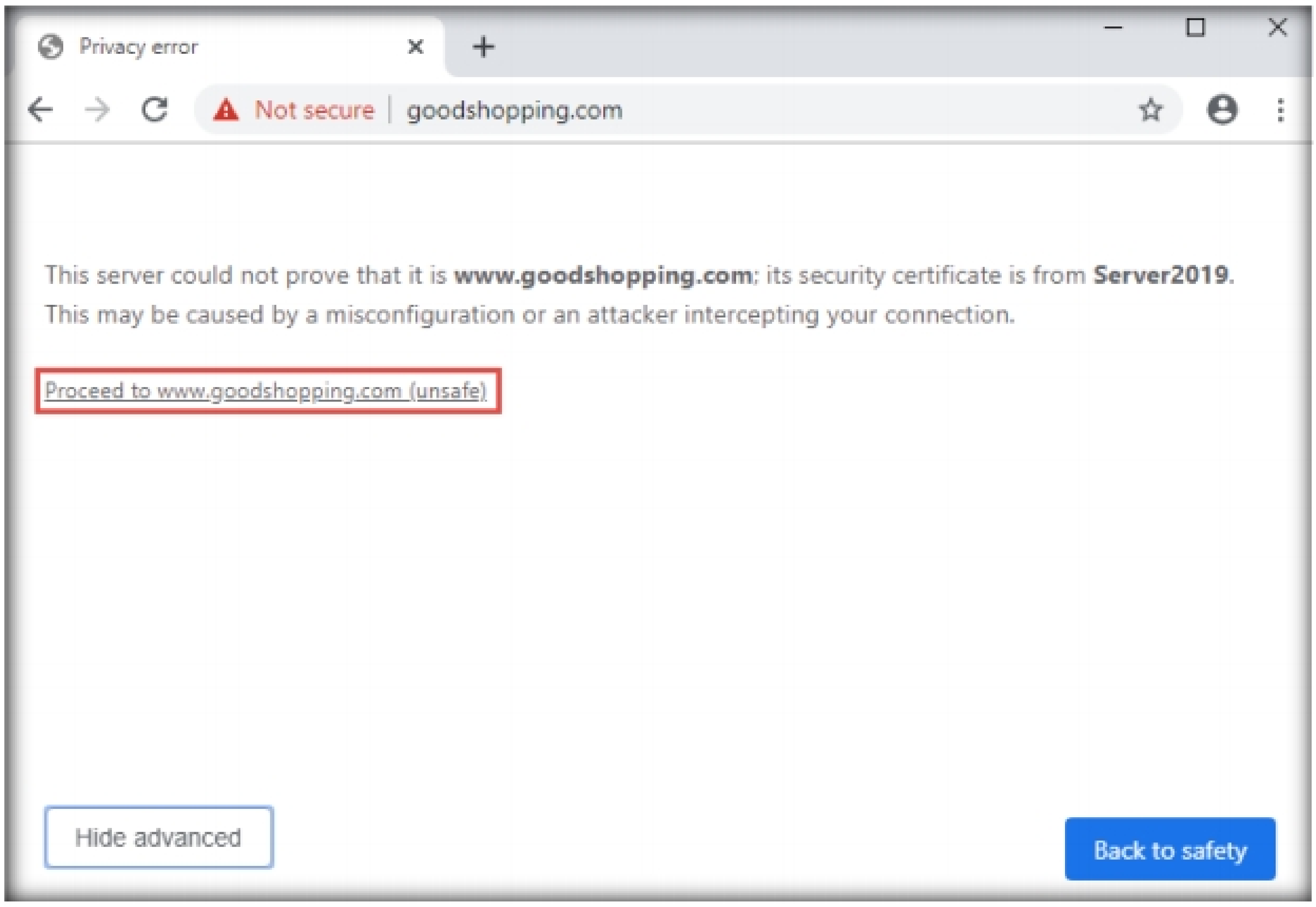
NET::ERR_CERT_COMMON_NAME_INVALID

☐ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Advanced
Back to safety

Figure 2.1.12: Connection is not Private

22. Click **Proceed to www.goodshopping.com (unsafe)**.


Privacy error
Not secure
goodshopping.com

This server could not prove that it is **www.goodshopping.com**; its security certificate is from **Server2019**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to www.goodshopping.com (unsafe)

Hide advanced
Back to safety

Figure 2.1.13: Proceed to Unsafe Page

23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.

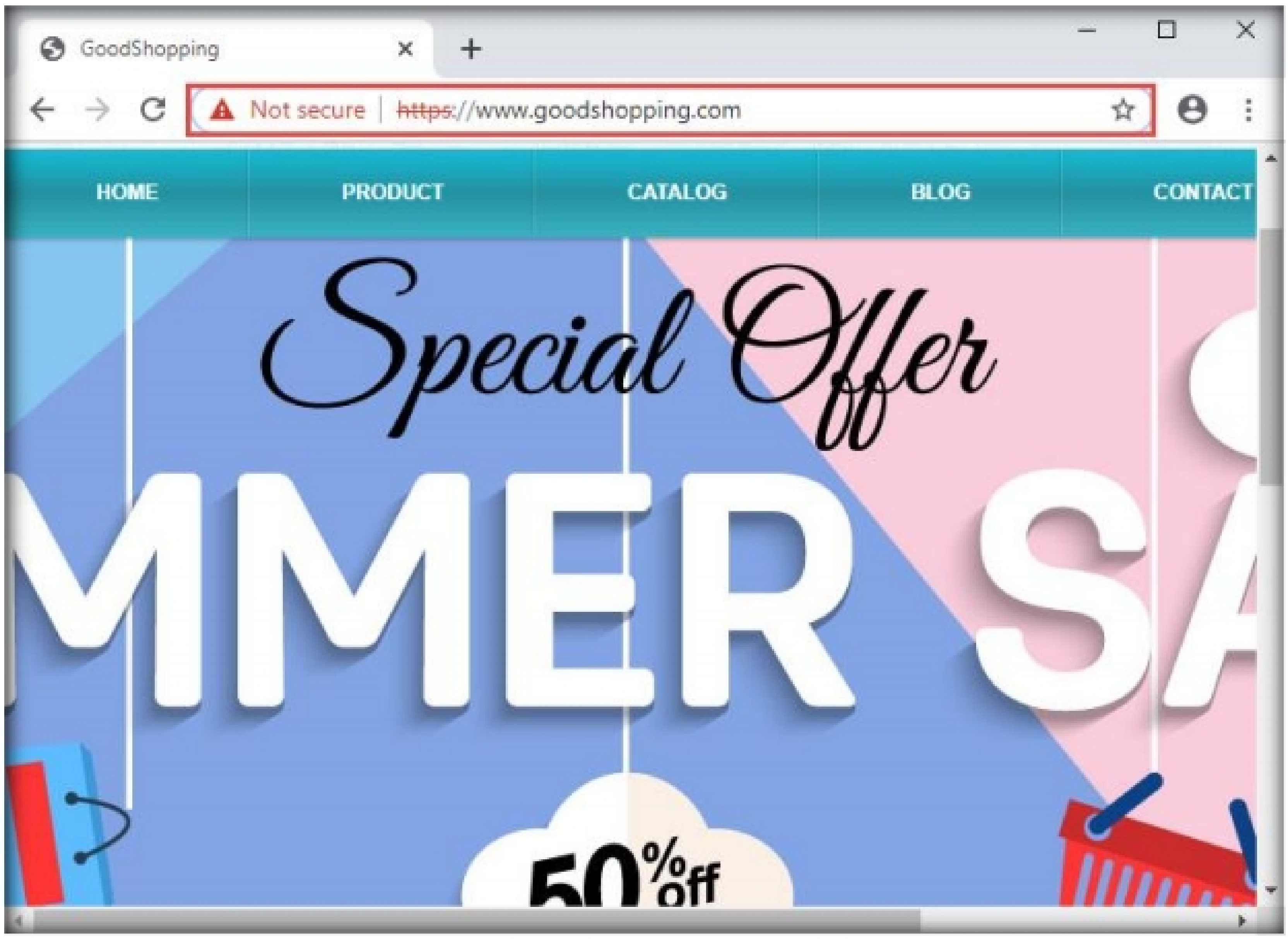

GoodShopping
Not secure | ~~https~~://www.goodshopping.com
HOME
PRODUCT
CATALOG
BLOG
CONTACT
Special Offer
MMER SA
50%off

Figure 2.1.14: Self-signed Certificate Page

24. This concludes the demonstration of creating and using a self-signed certificate.

25. Close all open windows and document all the acquired information.

26. Turn off the **Windows Server 2019** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 3

Perform Email Encryption

Email encryption is the process of encrypting email messages to protect the content from being viewed by entities other than the intended recipients.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Currently, the majority of businesses use email as their primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about an organization such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause huge losses to the organization. One can protect emails containing sensitive information by encrypting them.

As a professional ethical hacker and penetration tester, you must have proper knowledge of encrypting email messages so that sensitive information sent through emails remain intact. This lab will demonstrate how to encrypt email messages using various email encryption tools.

Lab Objectives

- Perform email encryption using RMail

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Duration

Time: 10 Minutes

Overview of Email Encryption

Email encryption hides the email content from eavesdroppers by encrypting it into an unreadable form. Emails can be encrypted and decrypted by means of a digital signature mechanism that uses public and private keys: the public key is shared, while the private key is kept private.

There are numerous methods that can be employed for email encryption, including:

- **Digital Signature**: Uses asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- **Secure Sockets Layer (SSL)**: Uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections
- **Transport Layer Security (TLS)**: Uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- **Pretty Good Privacy (PGP)**: Used to encrypt and decrypt data that provides authentication and cryptographic privacy
- **GNU Privacy Guard (GPG)**: Software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data

Lab Tasks

TASK 1

Perform Email Encryption using RMail

Here, we will use the RMail tool to perform email encryption.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Create an Account in the RMail Website

3. Open any web browser (here, **Google Chrome**), type **https://www.rmail.com/free-trial/** in the address bar, and press **Enter**.
4. The **RMail FREE TRIAL** webpage appears, as well as the registration form. Fill in the required personal details.

RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

5. Check the **I'm not a robot** checkbox and click **Start Free Trial**.

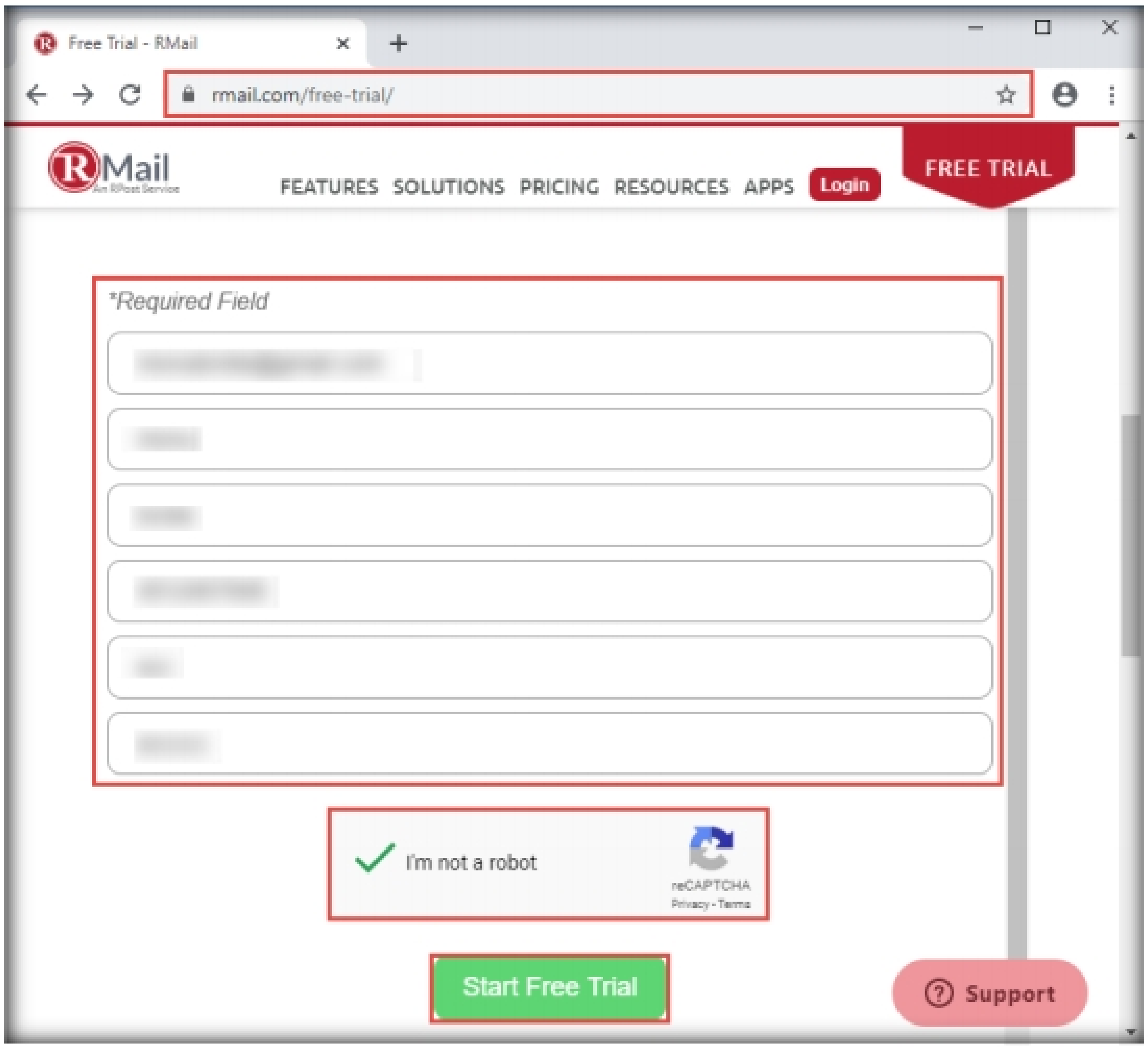
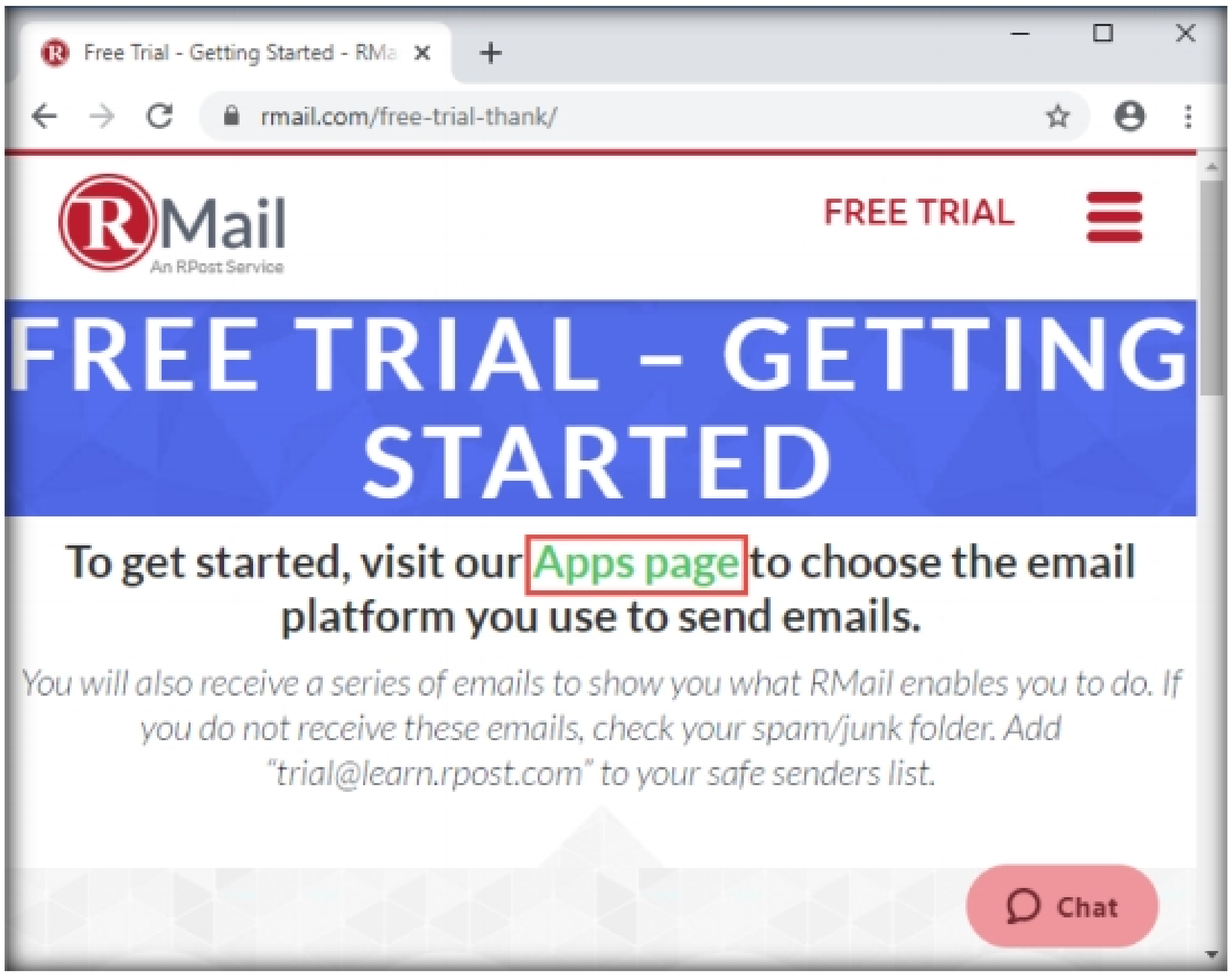

Free Trial - RMail
rmail.com/free-trial/
RMail
FEATURES SOLUTIONS PRICING RESOURCES APPS Login
FREE TRIAL
*Required Field
I'm not a robot
reCAPTCHA
Privacy - Terms
Start Free Trial
Support

Figure 3.1.1: FREE TRIAL registration form

6. The **FREE TRIAL - GETTING STARTED** page appears; click **Apps page** hyperlink.


Free Trial - Getting Started - RMa
rmail.com/free-trial-thank/
RMail
An RPost Service
FREE TRIAL
FREE TRIAL – GETTING STARTED

To get started, visit our Apps page to choose the email platform you use to send emails.

You will also receive a series of emails to show you what RMail enables you to do. If you do not receive these emails, check your spam/junk folder. Add "trial@learn.rpost.com" to your safe senders list.

Chat

Figure 3.1.2: FREE TRIAL - GETTING STARTED page

TASK 1.2

Add RMail to the Gmail

7. The **APPS & DOWNLOADS** page appears; click the **RMail for Gmail (Chrome)** option from the available platforms.

Note: In this task, we will be using the Gmail platform to demonstrate the working of RMail. However, you can use RMail on the platform of your choice.

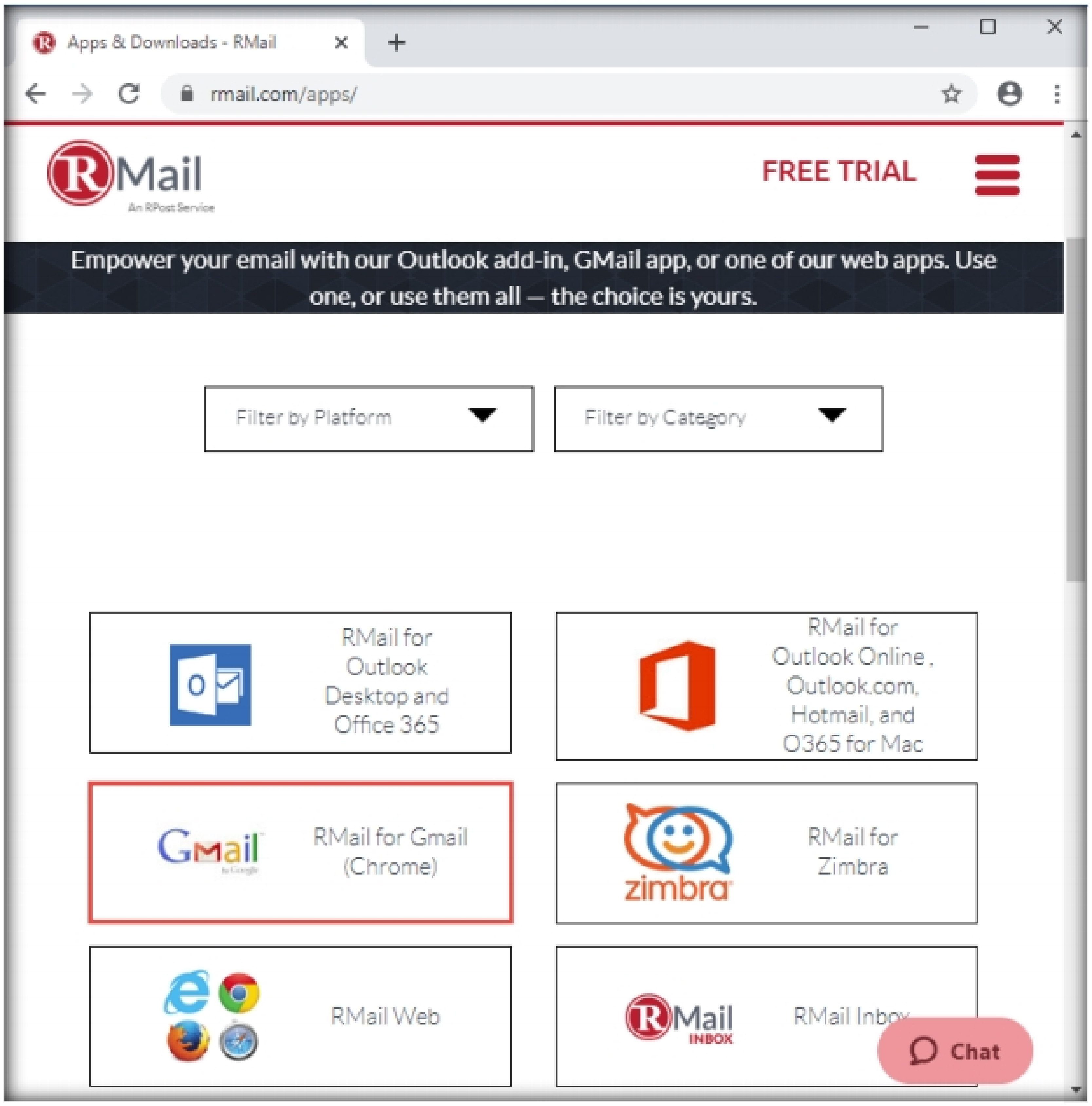
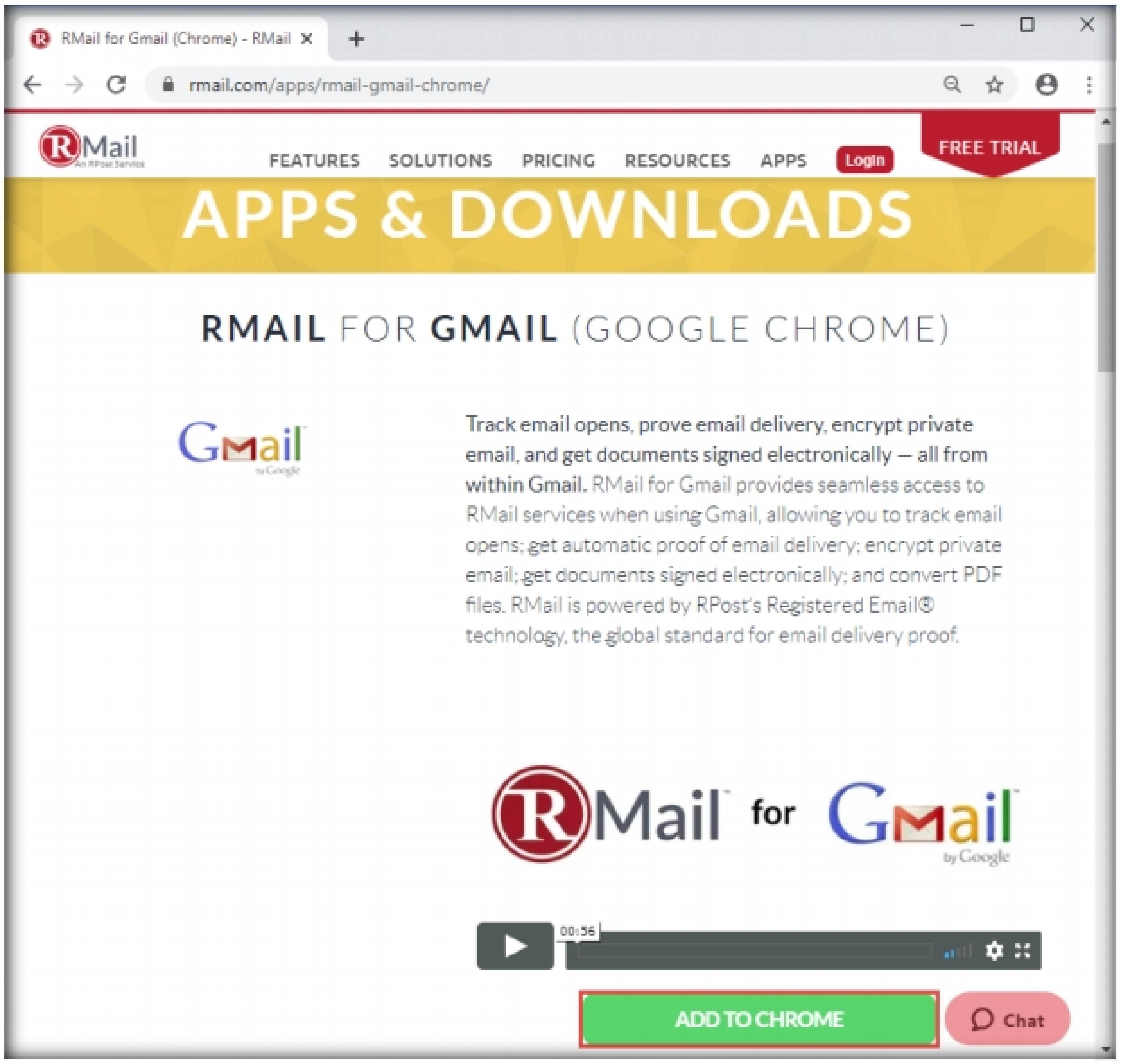

Apps & Downloads - RMail
rmail.com/apps/
RMail
An RPost Service
FREE TRIAL
Empower your email with our Outlook add-in, GMail app, or one of our web apps. Use one, or use them all — the choice is yours.
Filter by Platform
Filter by Category
RMail for Outlook Desktop and Office 365
RMail for Outlook Online , Outlook.com, Hotmail, and O365 for Mac
Gmail
RMail for Gmail (Chrome)
zimbra
RMail for Zimbra
RMail Web
RMail INBOX
RMail Inbox
Chat

Figure 3.1.3: APPS & DOWNLOADS page

8. The **RMAIL FOR GMAIL (GOOGLE CHROME)** page appears; scroll down and click the **ADD TO CHROME** button.



RMail for Gmail (Chrome) - RMail
rmail.com/apps/rmail-gmail-chrome/
FEATURES
SOLUTIONS
PRICING
RESOURCES
APPS
Login
FREE TRIAL
APPS & DOWNLOADS
RMAIL FOR GMAIL (GOOGLE CHROME)
00:56
ADD TO CHROME
Chat

Track email opens, prove email delivery, encrypt private email, and get documents signed electronically — all from within Gmail. RMail for Gmail provides seamless access to RMail services when using Gmail, allowing you to track email opens; get automatic proof of email delivery; encrypt private email; get documents signed electronically; and convert PDF files. RMail is powered by RPost's Registered Email® technology, the global standard for email delivery proof.

Figure 3.1.4: RMAIL FOR GMAIL (GOOGLE CHROME) page

9. A **chrome web store** page appears; click the **Add to Chrome** button under the **RPost for Gmail** option.

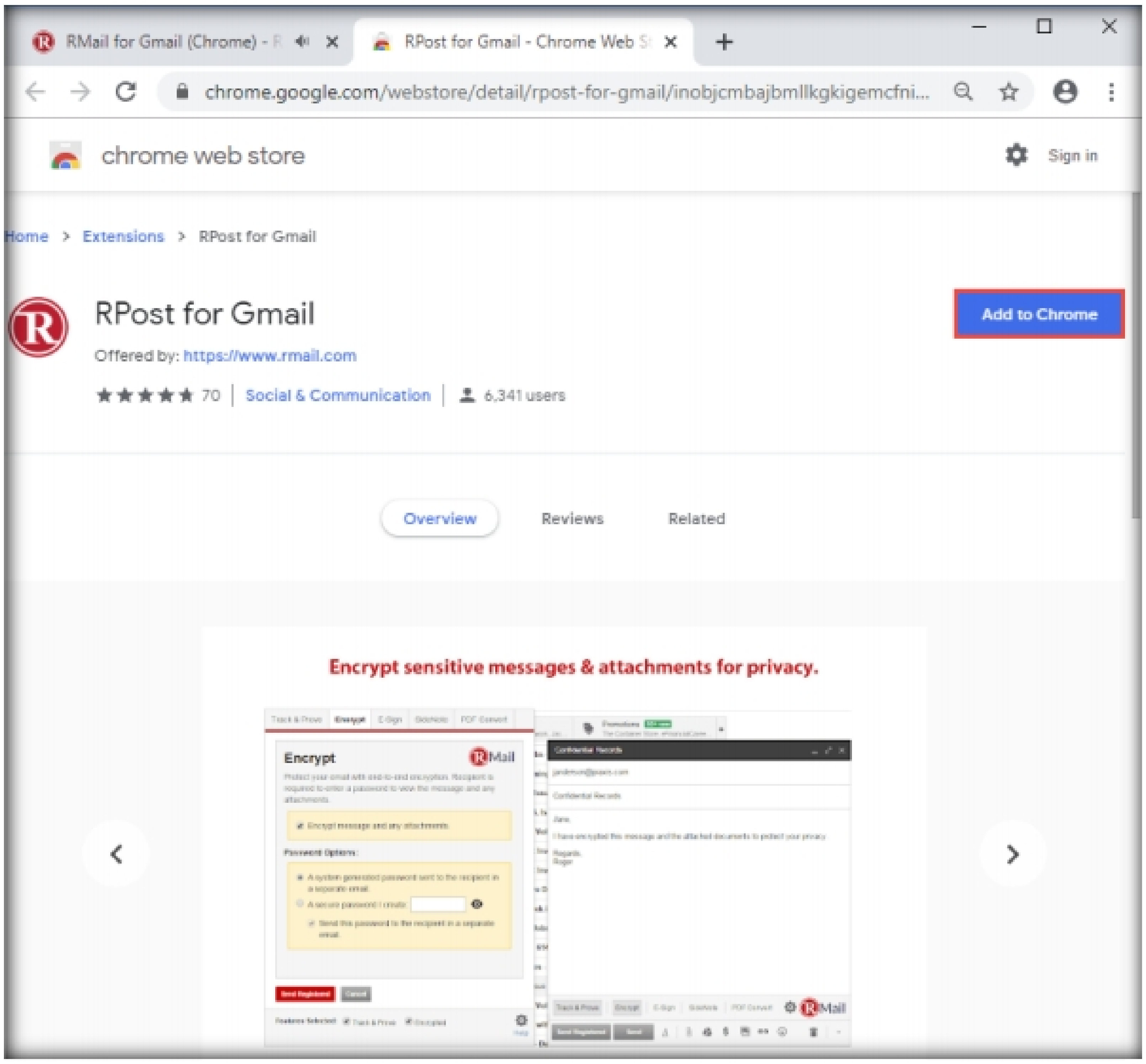
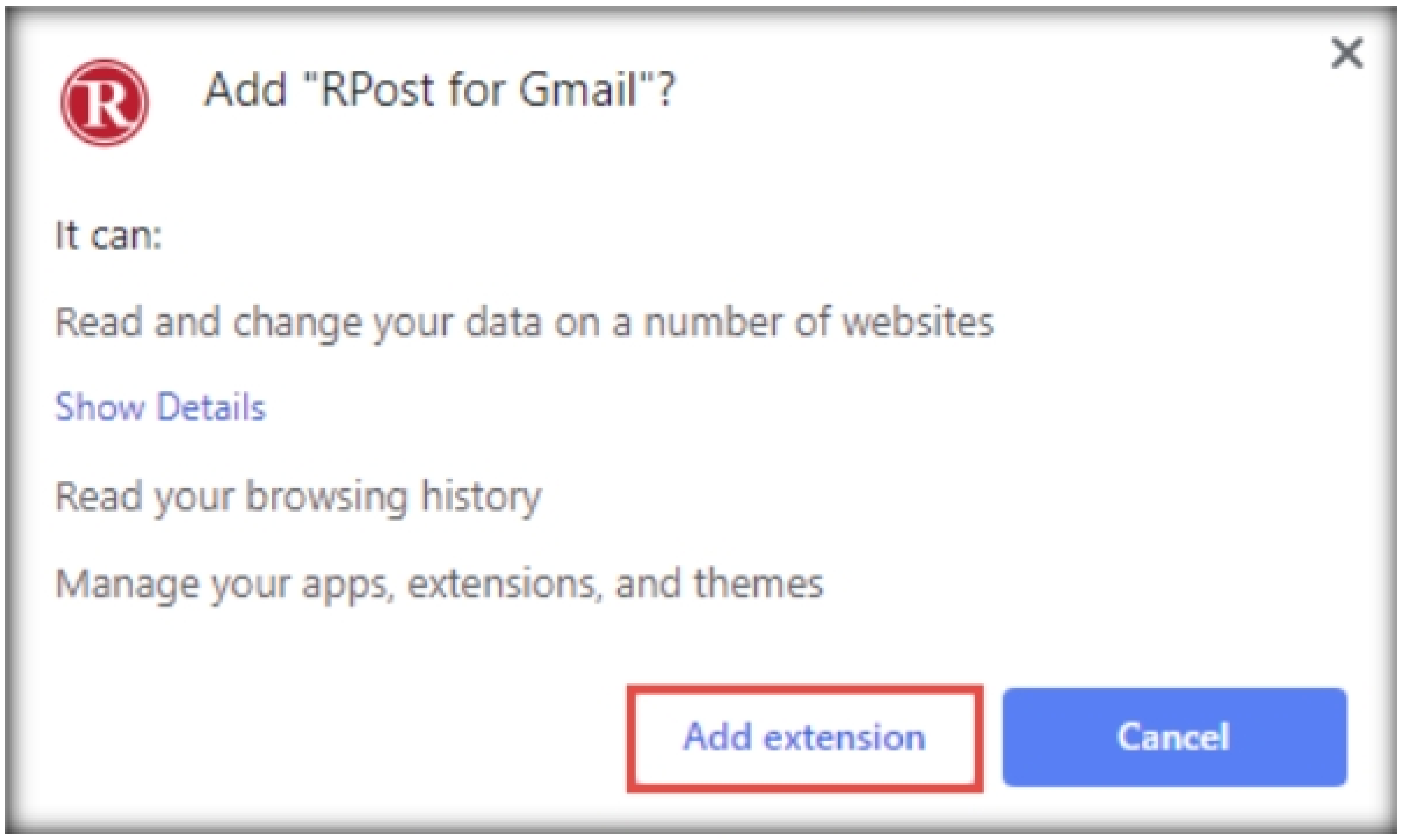

RMail for Gmail (Chrome) - R
RPost for Gmail - Chrome Web S
chrome.google.com/webstore/detail/rpost-for-gmail/inobjcmbajbmllkgkigemcfni...
chrome web store
Sign in
Home > Extensions > RPost for Gmail
RPost for Gmail
Offered by: https://www.rmail.com
70
Social & Communication
6,341 users
Add to Chrome
Overview
Reviews
Related
Encrypt sensitive messages & attachments for privacy.
Encrypt

Figure 3.1.5: chrome web store page

10. The **Add "RPost for Gmail"?** notification appears; click **Add extension**.


Add "RPost for Gmail"?

It can:

Read and change your data on a number of websites

Show Details

Read your browsing history

Manage your apps, extensions, and themes

Add extension
Cancel

Figure 3.1.6: Add "RPost for Gmail"? notification

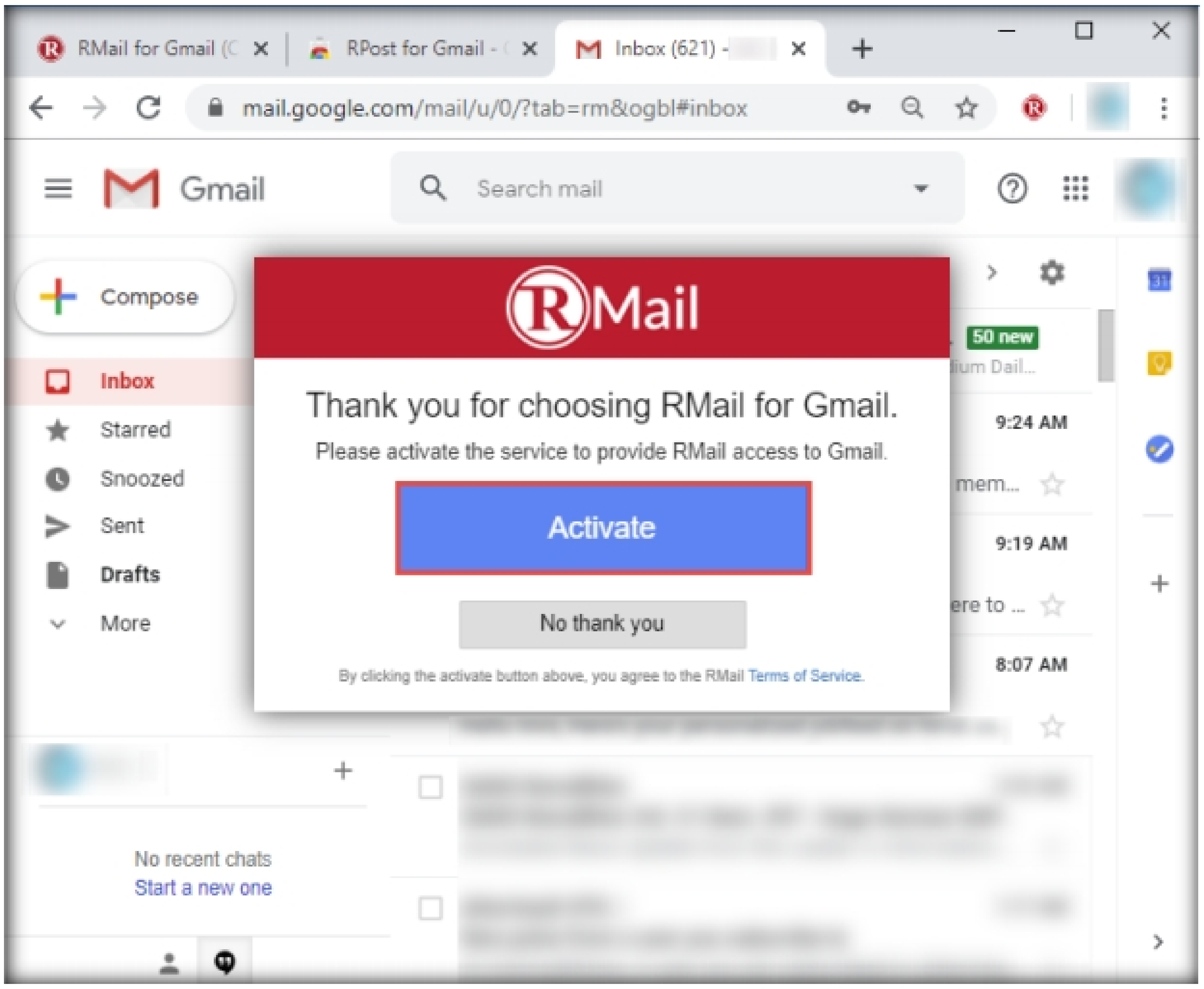
11. **RPost** is added to the browser and an **RPost for Gmail has been added to Chrome** notification appears.

12. Now, open a new tab in the browser and open the **Gmail** account within which you wish to implement email encryption.

TASK 1.3

Set RMail in your Gmail Account

13. Once you log in to your **Gmail** account, the **RMail** pop-up appears. Click the **Activate** button.


RMail for Gmail (C
RPost for Gmail - (
Inbox (621) -
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox
Gmail
Search mail
Compose
Inbox
Starred
Snoozed
Sent
Drafts
More
No recent chats
Start a new one
RMail
Activate
No thank you
50 new
9:24 AM
9:19 AM
8:07 AM

Thank you for choosing RMail for Gmail.

Please activate the service to provide RMail access to Gmail.

By clicking the activate button above, you agree to the RMail Terms of Service.

Figure 3.1.7: Adding RMail to the account

14. The **Sign in - Google Accounts** page appears; under the **Choose an account**, click on your account.

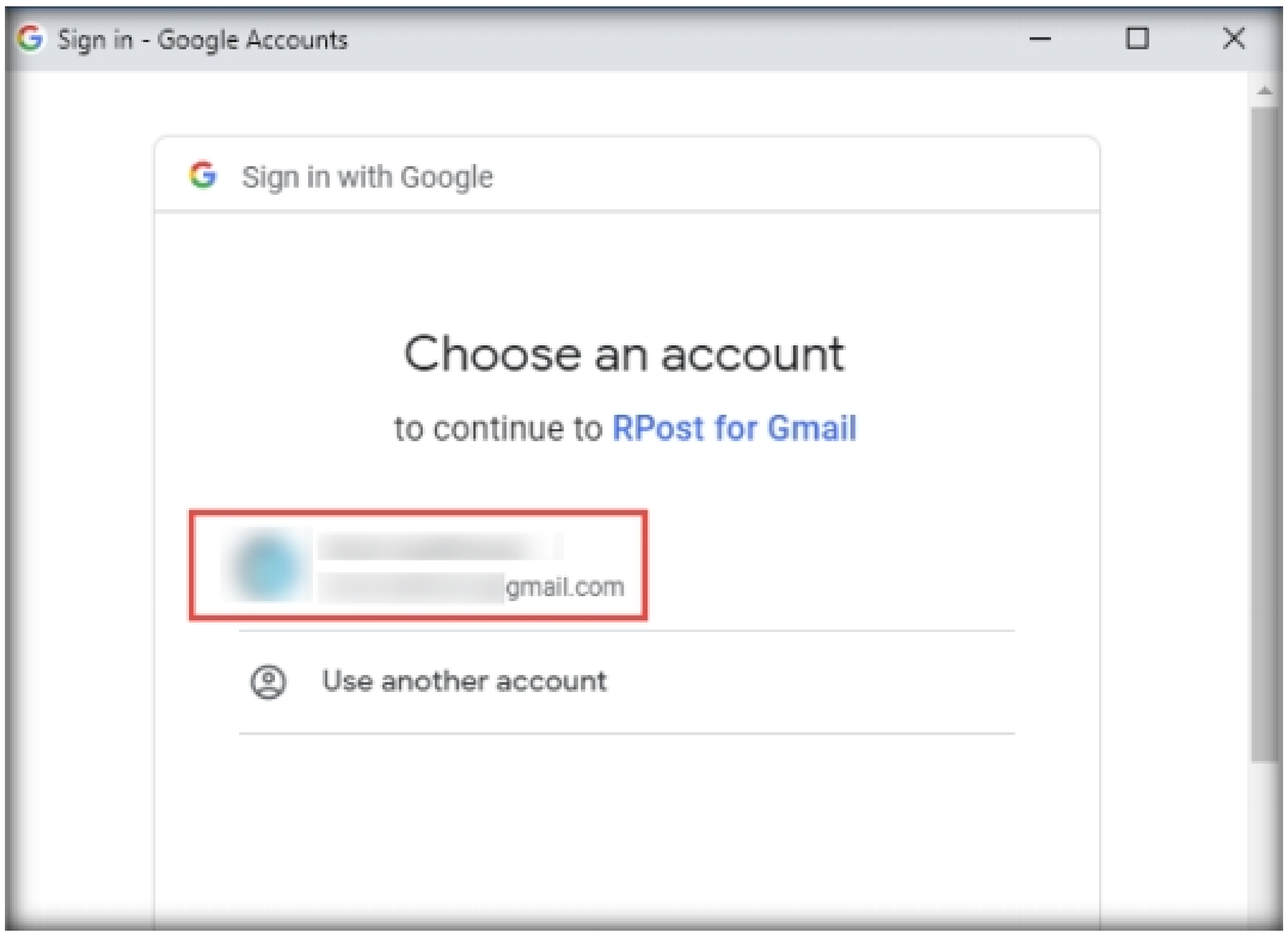
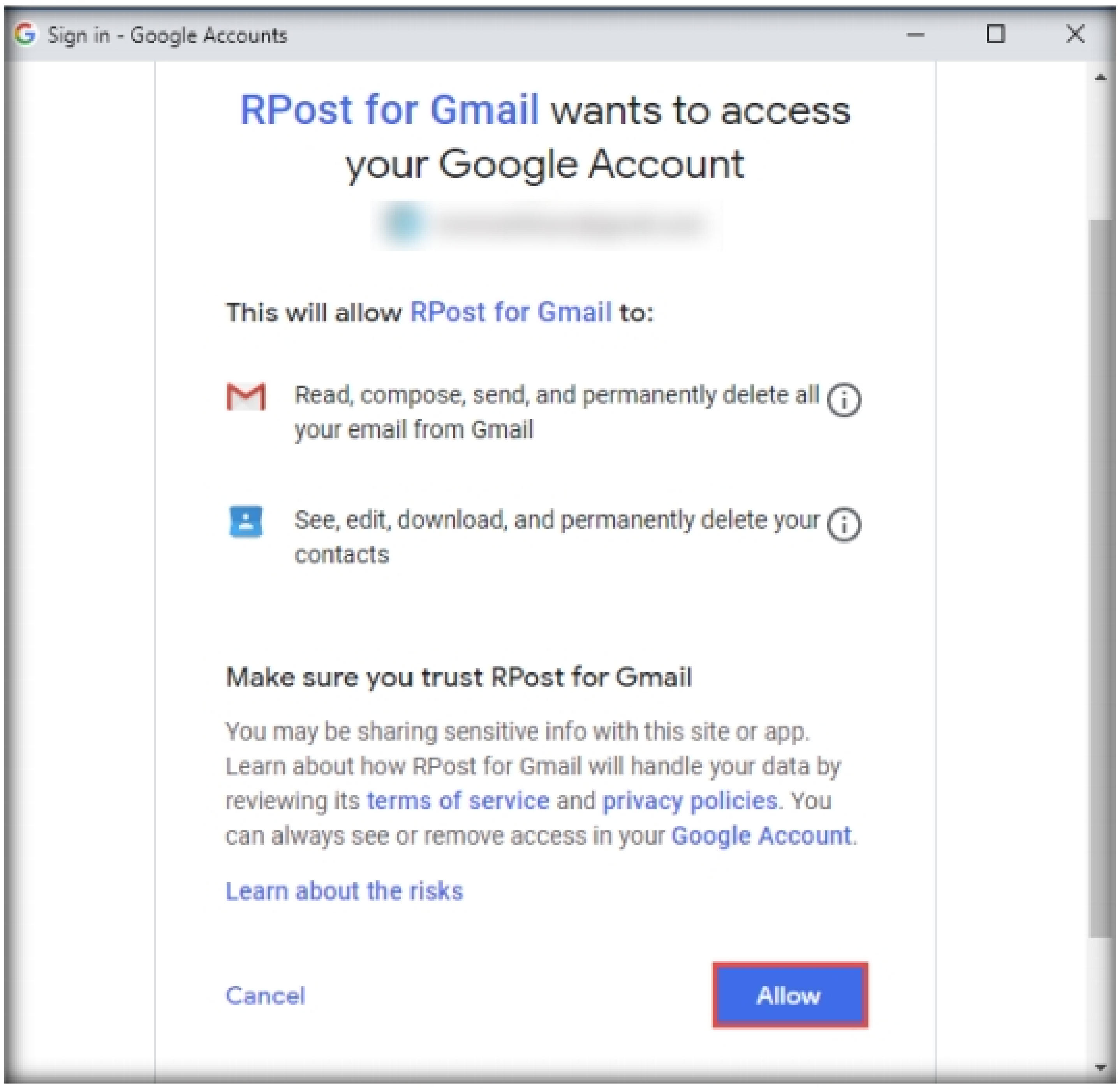

Sign in - Google Accounts
Sign in with Google
Choose an account
to continue to RPost for Gmail
gmail.com
Use another account

Figure 3.1.8: Sign in - Google Account page

15. The **RPost for Gmail wants to access your Google Account** wizard appears; click the **Allow** button.


Sign in - Google Accounts
Cancel
Allow

RPost for Gmail wants to access your Google Account

This will allow RPost for Gmail to:

Read, compose, send, and permanently delete all your email from Gmail

See, edit, download, and permanently delete your contacts

Make sure you trust RPost for Gmail

You may be sharing sensitive info with this site or app. Learn about how RPost for Gmail will handle your data by reviewing its terms of service and privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

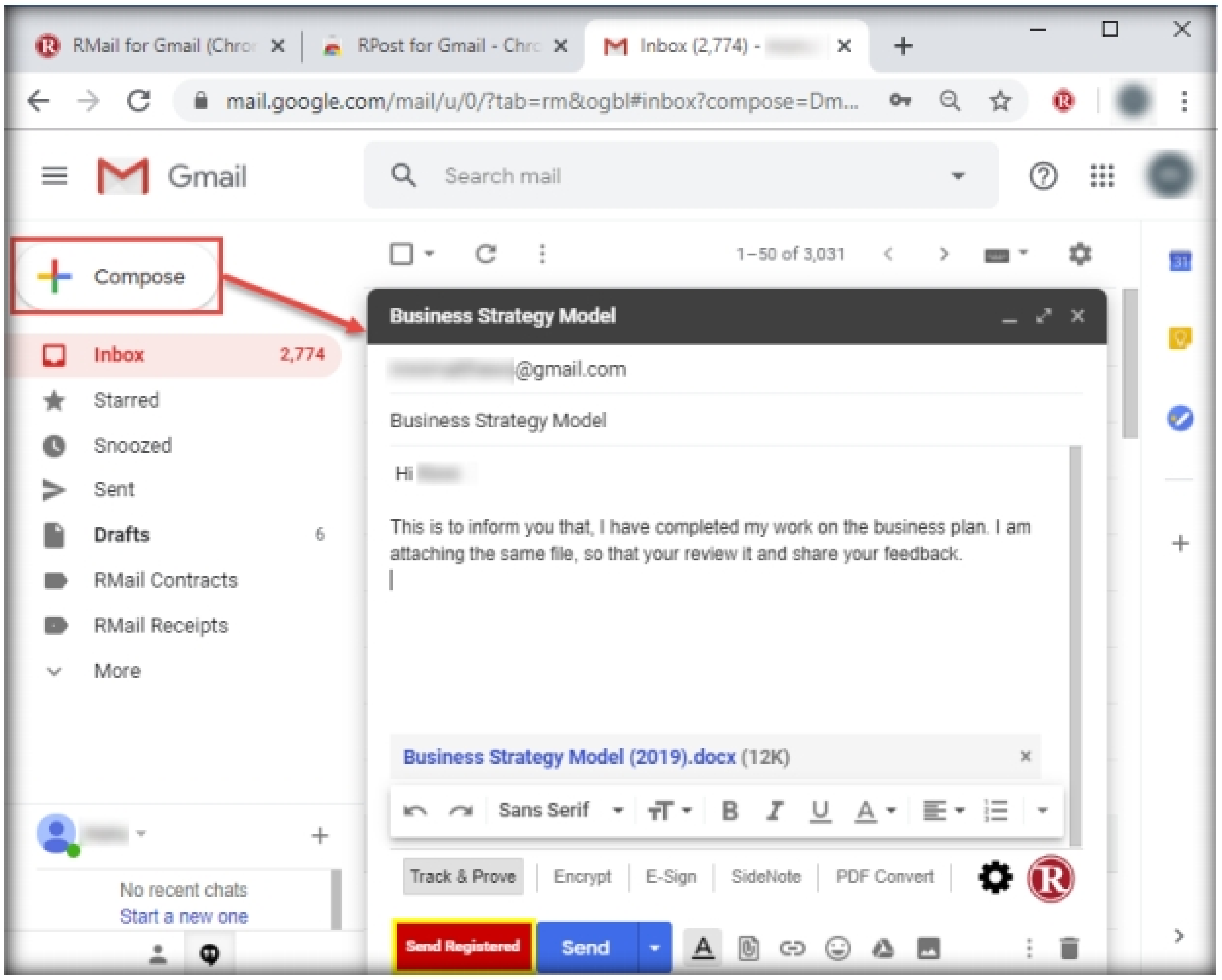
Figure 3.1.9: RPost for Gmail wants to access your Google Account wizard

16. The **Thank you For Choosing RMail** page appears. Close the tab and navigate back to your **Gmail** account page.

TASK 1.4

Compose an Email

17. Click **Compose** from the left-hand pane; the email body appears. Compose an email and click **Send Registered**.


RMail for Gmail (Chro
RPost for Gmail - Chro
Inbox (2,774) - [redacted]
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox?compose=Dm...
Gmail
Search mail
Compose
1–50 of 3,031
Inbox 2,774
Starred
Snoozed
Sent
Drafts 6
RMail Contracts
RMail Receipts
More
No recent chats
Start a new one
Sans Serif
Track & Prove
Encrypt
E-Sign
SideNote
PDF Convert
Send Registered
Send

Business Strategy Model

[redacted]@gmail.com

Business Strategy Model

Hi [redacted]

This is to inform you that, I have completed my work on the business plan. I am attaching the same file, so that your review it and share your feedback.

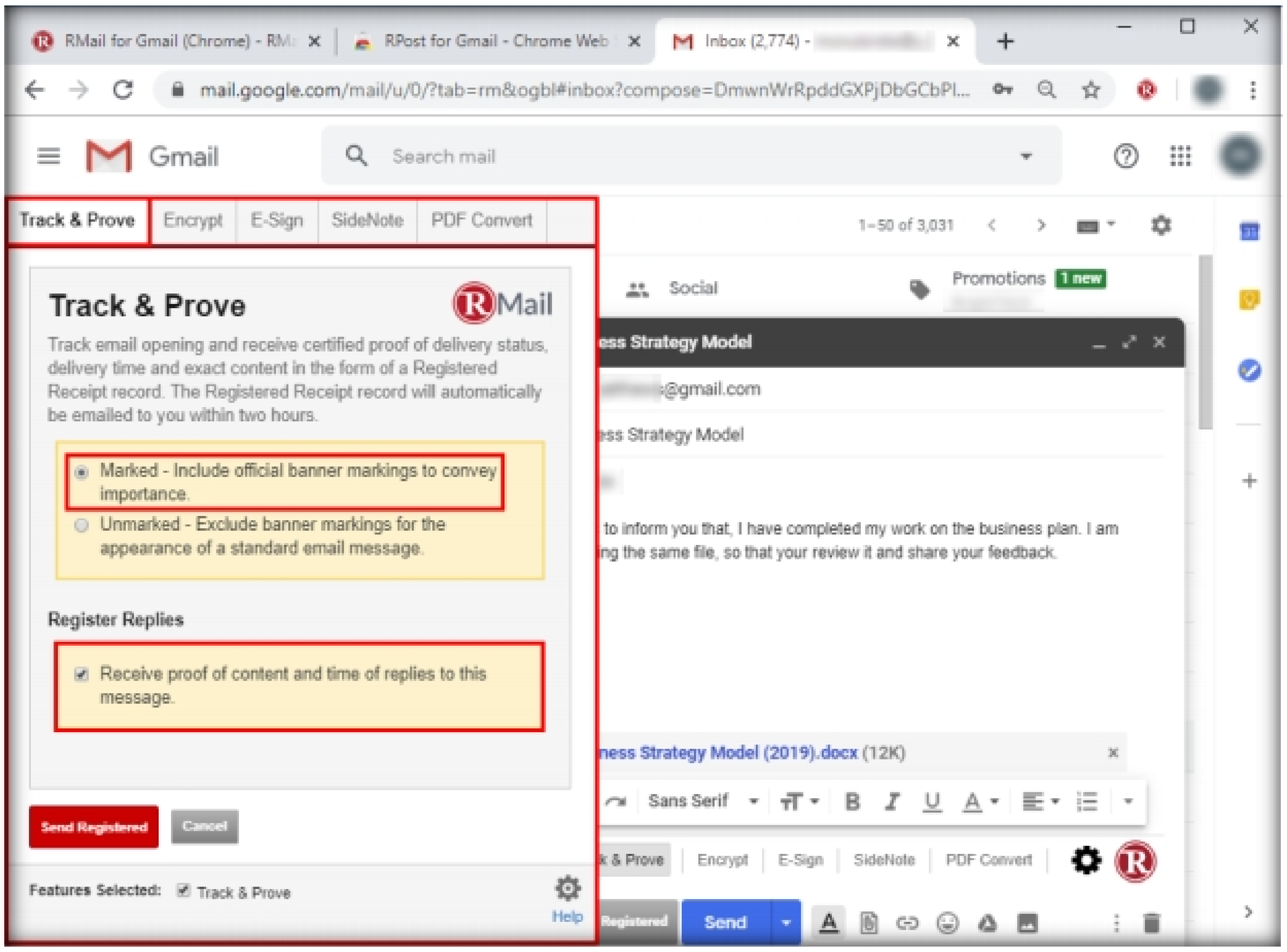
Business Strategy Model (2019).docx (12K)

Figure 3.1.10: Compose an email

TASK 1.5

Set RMail Options and Sent an Email

18. The RMail **Track & Prove** pop-up appears; ensure that the **Marked** radio button is selected. Under the **Register Replies** section, check the **Receive proof of content and time of replies to this message** checkbox. Then, click the **Encrypt** tab.



Track & Prove | Encrypt | E-Sign | SideNote | PDF Convert

Track & Prove

Track email opening and receive certified proof of delivery status, delivery time and exact content in the form of a Registered Receipt record. The Registered Receipt record will automatically be emailed to you within two hours.

● Marked - Include official banner markings to convey importance.

○ Unmarked - Exclude banner markings for the appearance of a standard email message.

Register Replies

☑ Receive proof of content and time of replies to this message.

Features Selected: ☑ Track & Prove

ess Strategy Model

[redacted]@gmail.com

ess Strategy Model

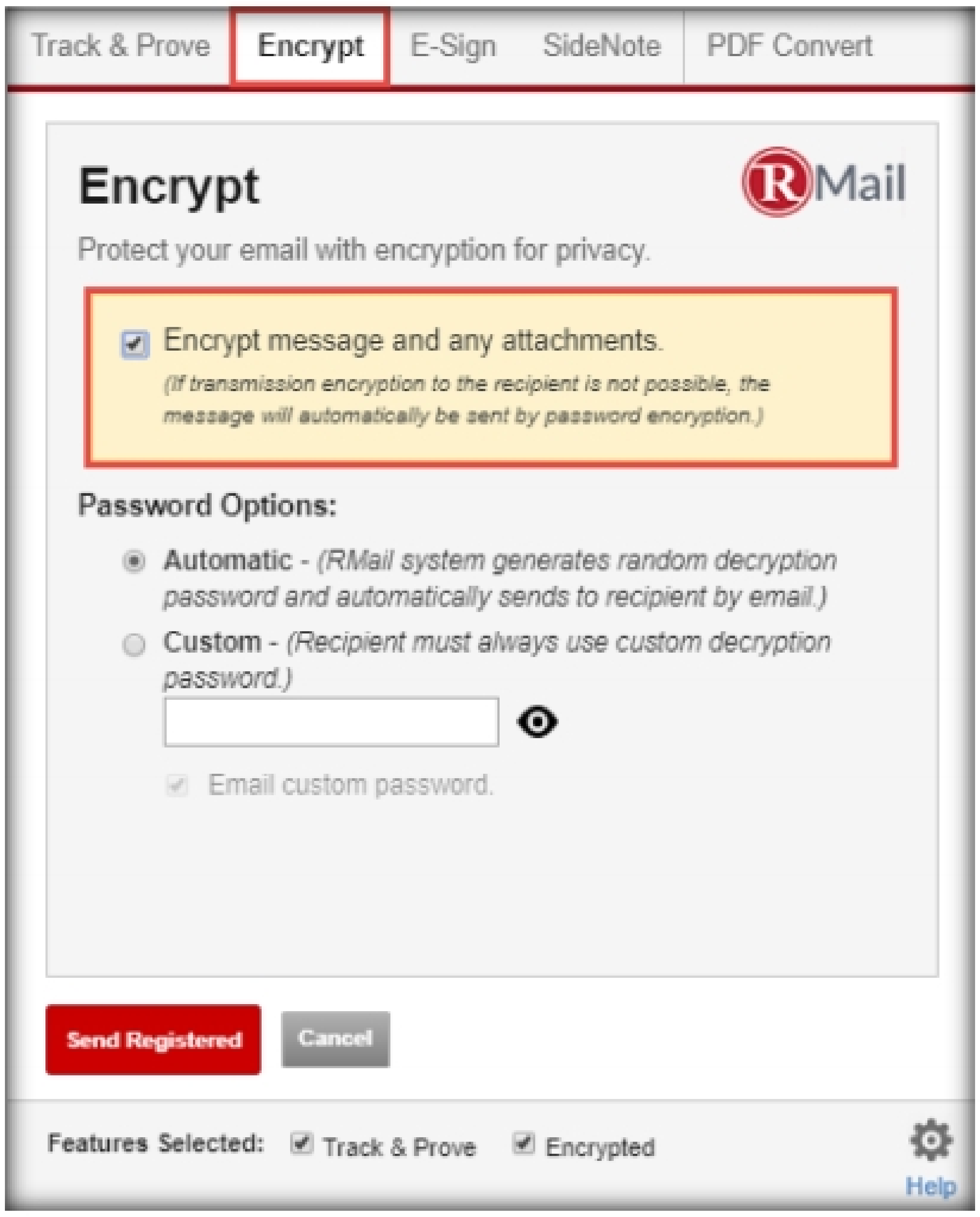
to inform you that, I have completed my work on the business plan. I am
ng the same file, so that your review it and share your feedback.

ness Strategy Model (2019).docx (12K)

RMail for Gmail (Chrome) - RM
RPost for Gmail - Chrome Web
Inbox (2,774) -
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox?compose=DmwnWrRpddGXPjDbGCbPl...
Gmail
Search mail
1–50 of 3,031
Social
Promotions
1 new
Sans Serif
Send Registered
Cancel
Help
Registered
Send

Figure 3.1.11: Track & Prove tab

19. In the **Encrypt** tab, check the **Encrypt message and any attachments** checkbox and click the **E-sign** tab.



Track & Prove | Encrypt | E-Sign | SideNote | PDF Convert

Encrypt

Protect your email with encryption for privacy.

☑ Encrypt message and any attachments.

(If transmission encryption to the recipient is not possible, the message will automatically be sent by password encryption.)

Password Options:

● **Automatic** - *(RMail system generates random decryption password and automatically sends to recipient by email.)*

○ **Custom** - *(Recipient must always use custom decryption password.)*

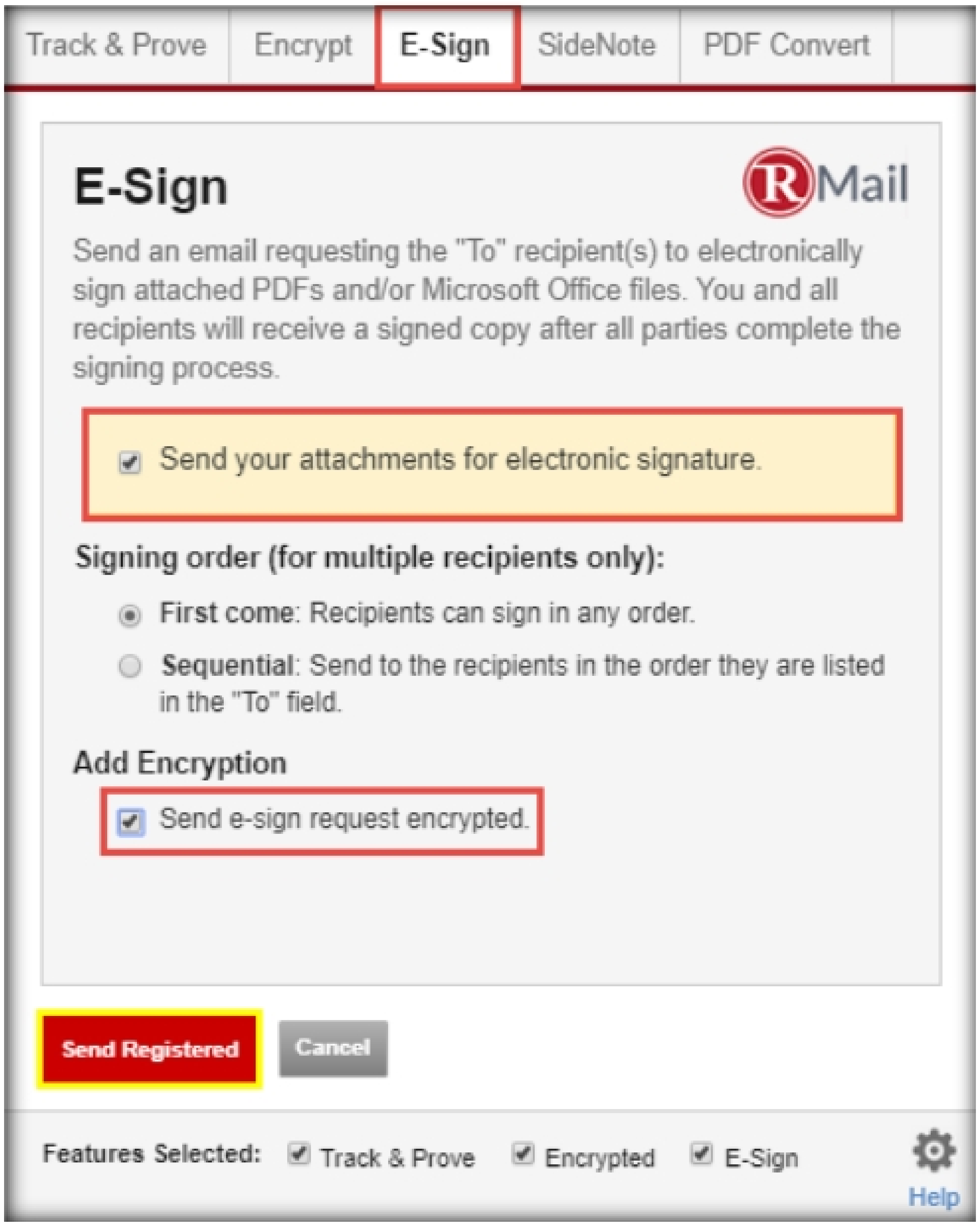
☑ Email custom password.

Features Selected: ☑ Track & Prove ☑ Encrypted

RMail
Send Registered
Cancel
Help

Figure 3.1.12: Encrypt tab

20. In the **E-Sign** tab, check both the **Send your attachments for electronic signature** and **Send e-sign request encrypted** checkboxes. Click the **Send Registered** button.



Send an email requesting the "To" recipient(s) to electronically sign attached PDFs and/or Microsoft Office files. You and all recipients will receive a signed copy after all parties complete the signing process.

☑ Send your attachments for electronic signature.

Signing order (for multiple recipients only):

● First come: Recipients can sign in any order.

○ Sequential: Send to the recipients in the order they are listed in the "To" field.

Add Encryption

☑ Send e-sign request encrypted.

Features Selected: ☑ Track & Prove ☑ Encrypted ☑ E-Sign

Figure 3.1.13: E-Sign tab

21. In the **Inbox**, you can observe an **Acknowledgement** email with **Proof of Sending**.

22. In this task, for the purpose of demonstration, we will open the recipient's account and view the email.

TASK 1.6

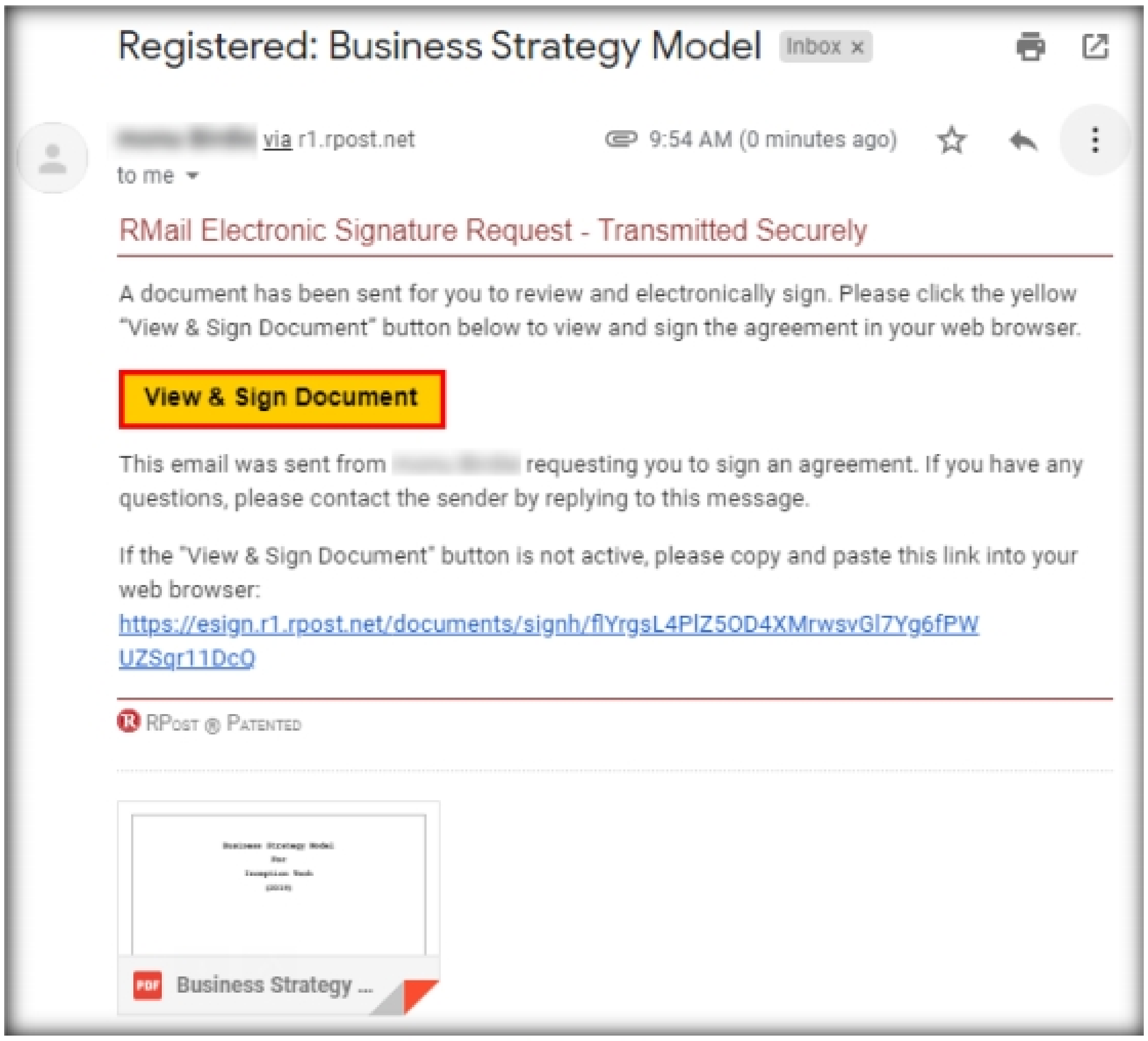
Login as Recipient

23. To do so, switch to the **Windows Server 2019** virtual machine and log in with **Administrator**/**Pa$$w0rd**.

24. Open any web browser (here, **Google Chrome**) and log in to the **Gmail** account of the recipient. Open the email from the sender.

25. You can observe that the email received is tagged as a registered email wherein a document has been sent for the recipient to review and electronically sign to confirm his/her identity.

26. Click the **View & Sign Document** button to sign an agreement.



Registered: Business Strategy Model

[redacted] via r1.rpost.net

to me

9:54 AM (0 minutes ago)

RMail Electronic Signature Request - Transmitted Securely

A document has been sent for you to review and electronically sign. Please click the yellow "View & Sign Document" button below to view and sign the agreement in your web browser.

View & Sign Document

This email was sent from [redacted] requesting you to sign an agreement. If you have any questions, please contact the sender by replying to this message.

If the "View & Sign Document" button is not active, please copy and paste this link into your web browser:
https://esign.r1.rpost.net/documents/signh/flYrgsL4PlZ5OD4XMrwsvGl7Yg6fPWUZSqr11DcQ

RPost ® Patented

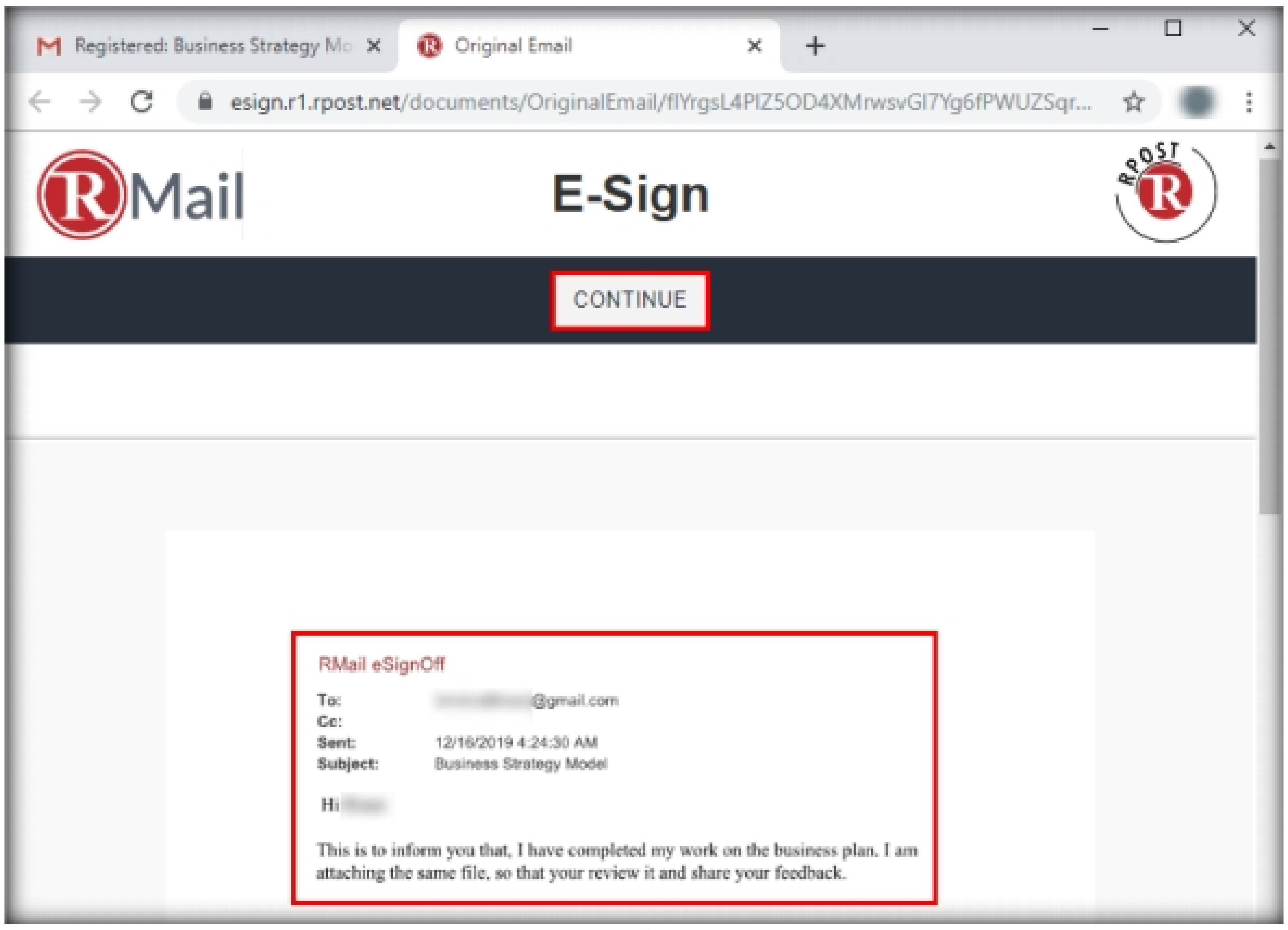
Inbox ×
Business Strategy ...

Figure 3.1.14: Email from the sender

TASK 1.7

E-Sign to Confirm Identity

27. A new **E-Sign** webpage appears displaying the email content; click **CONTINUE**.



Registered: Business Strategy Mo ×
Original Email ×
esign.r1.rpost.net/documents/OriginalEmail/flYrgsL4PlZ5OD4XMrwsvGl7Yg6fPWUZSqr...
RMail
E-Sign
RPOST
CONTINUE

RMail eSignOff

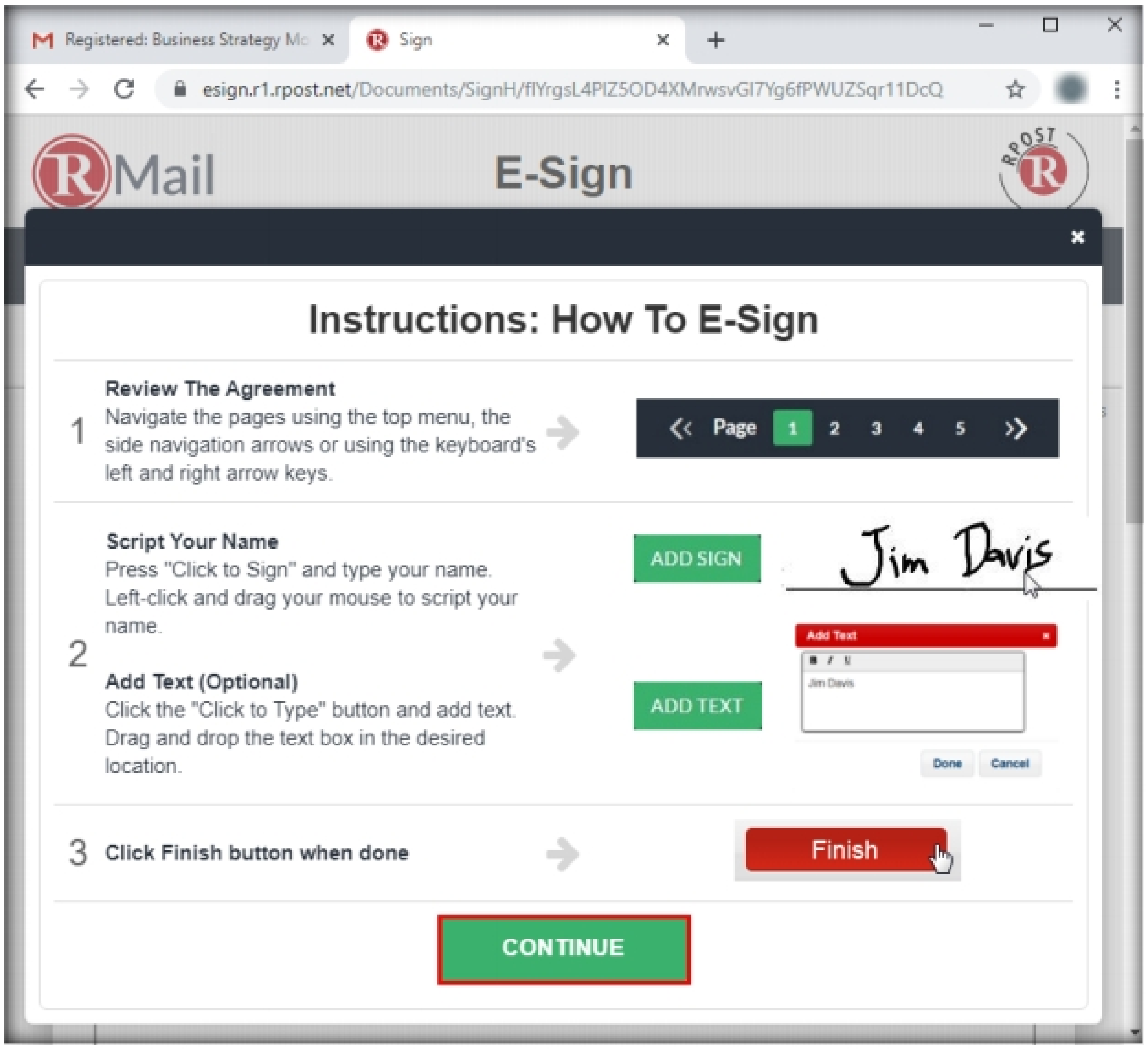
To: [redacted]@gmail.com
Cc:
Sent: 12/16/2019 4:24:30 AM
Subject: Business Strategy Model

Hi [redacted]

This is to inform you that, I have completed my work on the business plan. I am attaching the same file, so that your review it and share your feedback.

Figure 3.1.15: E-Sign page

28. The **Instructions: How To E-Sign** page appears; read the instructions carefully and click **CONTINUE**.



Instructions: How To E-Sign

1 **Review The Agreement**
Navigate the pages using the top menu, the side navigation arrows or using the keyboard's left and right arrow keys.

2 **Script Your Name**
Press "Click to Sign" and type your name. Left-click and drag your mouse to script your name.

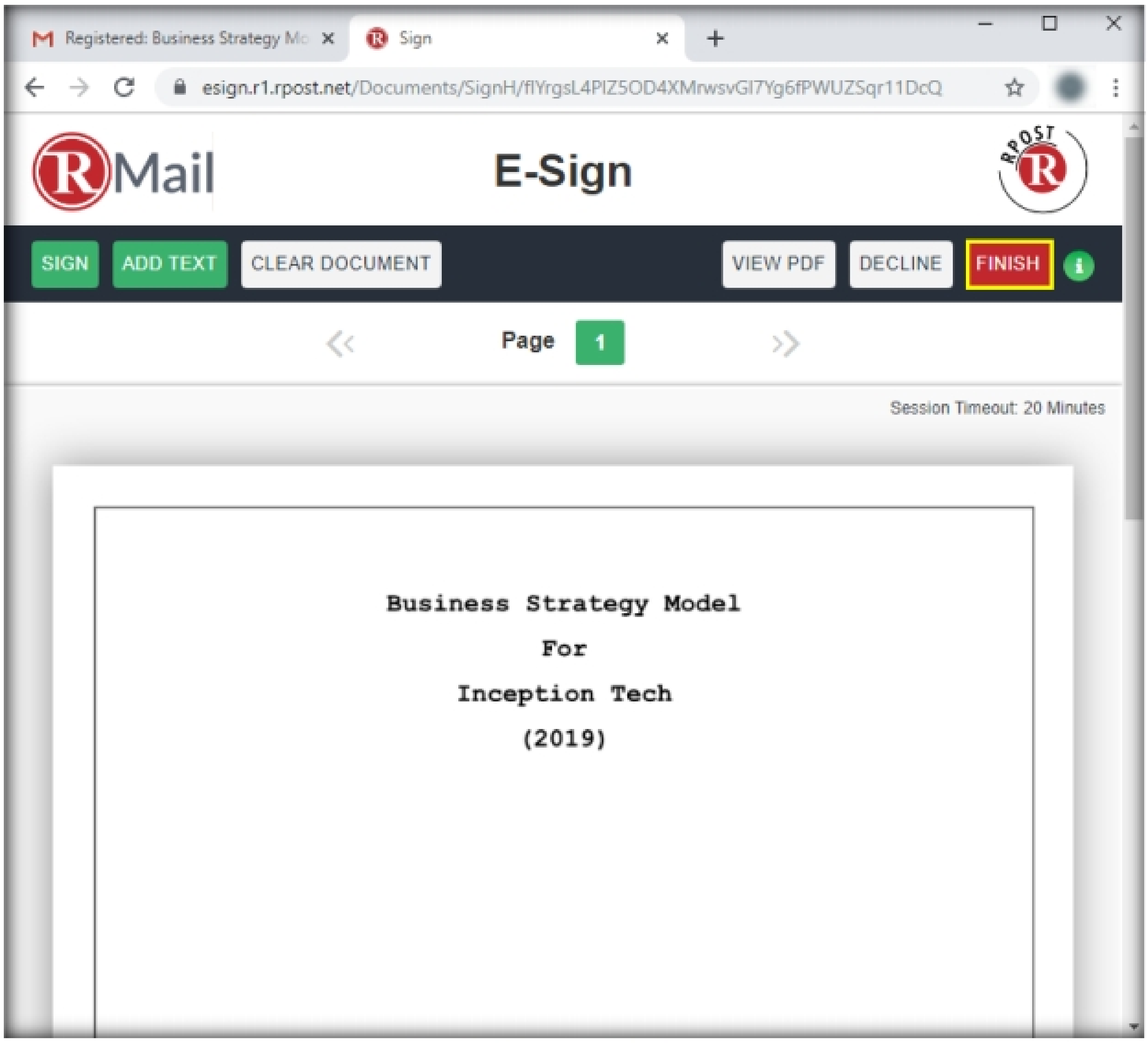
Add Text (Optional)
Click the "Click to Type" button and add text. Drag and drop the text box in the desired location.

3 **Click Finish button when done**

Registered: Business Strategy Mo
Sign
esign.r1.rpost.net/Documents/SignH/flYrgsL4PIZ5OD4XMrwsvGI7Yg6fPWUZSqr11DcQ
RMail
E-Sign
RPOST
Page 1 2 3 4 5
ADD SIGN
Jim Davis
ADD TEXT
Add Text
Jim Davis
Done
Cancel
Finish
CONTINUE

Figure 3.1.16: Instructions: How To E-Sign page

29. The attached document to the email (**Business Strategy Model (2019)**) appears, as shown in the screenshot.
30. After viewing the attached document, click **FINISH**.

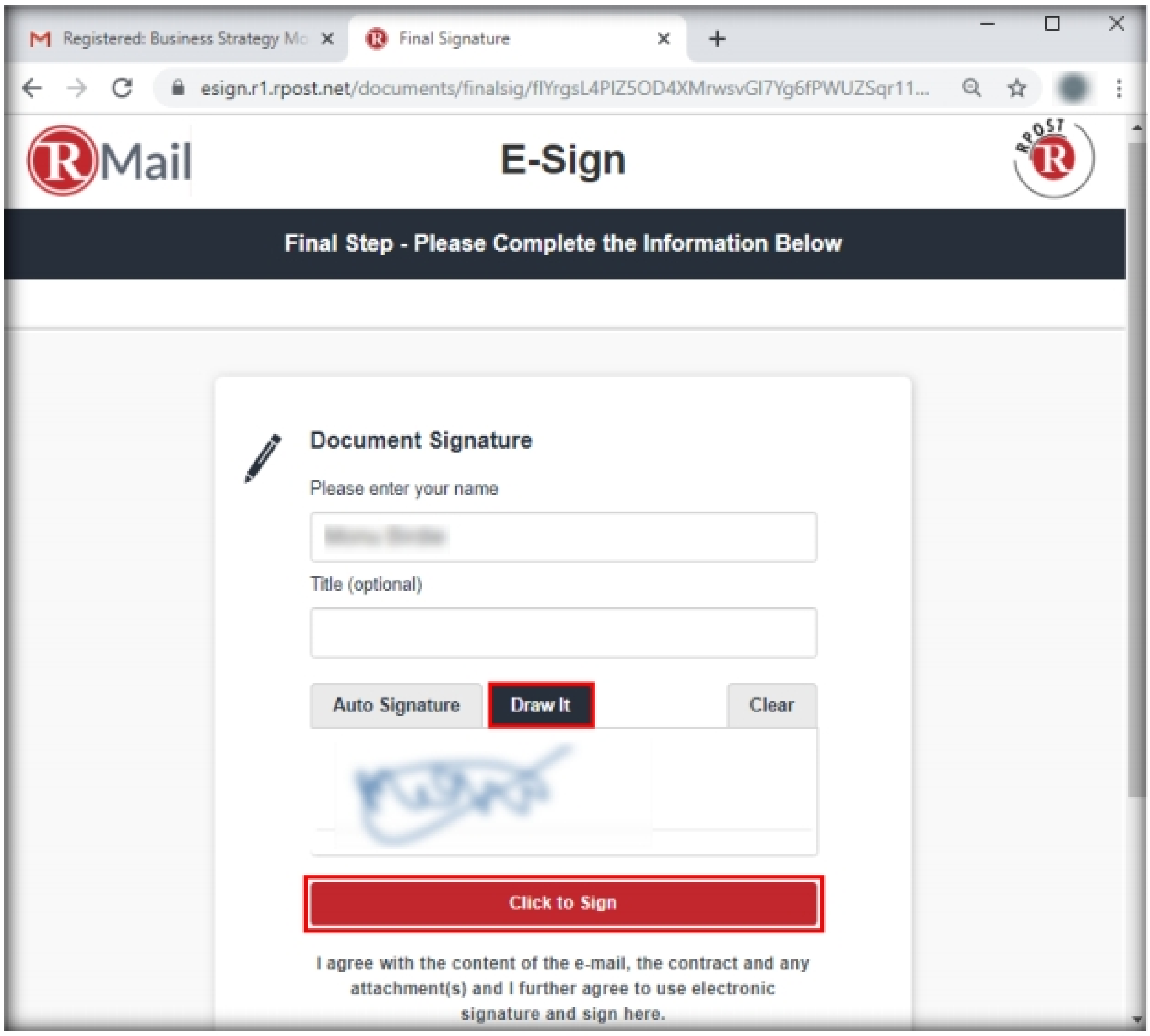

Registered: Business Strategy Mo
Sign
esign.r1.rpost.net/Documents/SignH/flYrgsL4PIZ5OD4XMrwsvGI7Yg6fPWUZSqr11DcQ
RMail
E-Sign
RPOST
SIGN
ADD TEXT
CLEAR DOCUMENT
VIEW PDF
DECLINE
FINISH
Page 1
Session Timeout: 20 Minutes

Business Strategy Model
For
Inception Tech
(2019)

Figure 3.1.17: Attached document

31. The **Final Step - Please Complete the Information Below** page appears with the **Document Signature** form. In the **Please enter your name** field, enter your name (Recipient's name) and leave the **Title** field blank.

32. Click the **Draw It** tab, sign in the field below and click the **Click to Sign** button.


Registered: Business Strategy Mo
Final Signature
esign.r1.rpost.net/documents/finalsig/flYrgsL4PIZ5OD4XMrwsvGI7Yg6fPWUZSqr11...
RMail
E-Sign
RPOST R

Final Step - Please Complete the Information Below

Document Signature

Please enter your name

Title (optional)

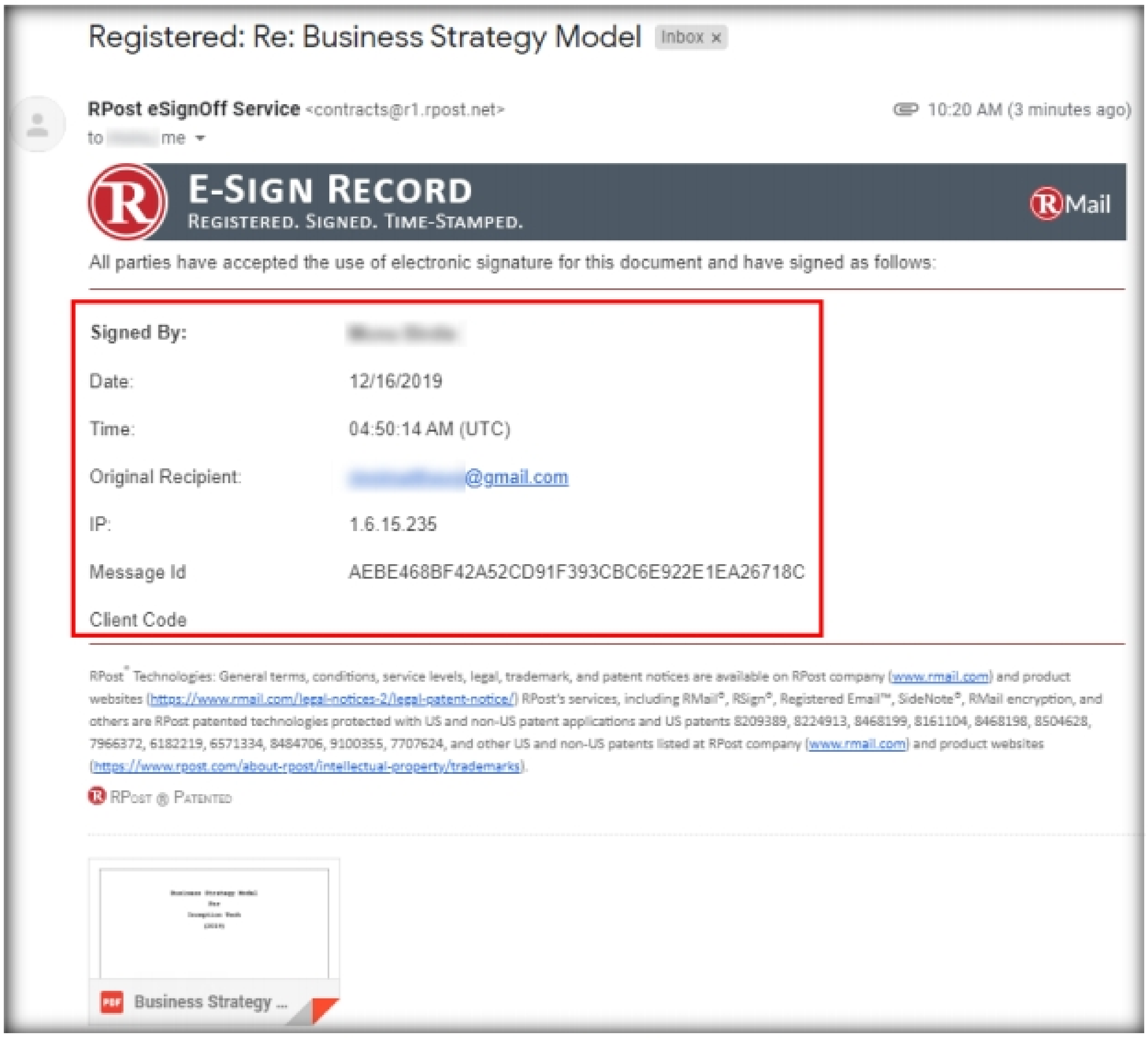
Auto Signature
Draw It
Clear
Click to Sign

I agree with the content of the e-mail, the contract and any attachment(s) and I further agree to use electronic signature and sign here.

Figure 3.1.18: Final Step: Please Complete the Information Below page

33. The **YOU'RE ALL DONE!** page appears; close the current tab to return to the opened email. Click **Inbox** from the left-hand pane to navigate to the inbox.

34. Open an email from **RPost eSignOff Service**. You can observe that it is an acknowledgment email from RPost along with various details such as **Signed By**, **Date**, **Time**, **Original Recipient**, **IP**, **Message Id**, etc.



Registered: Re: Business Strategy Model

RPost eSignOff Service <contracts@r1.rpost.net>
to [redacted] me
10:20 AM (3 minutes ago)

E-SIGN RECORD
REGISTERED. SIGNED. TIME-STAMPED.

All parties have accepted the use of electronic signature for this document and have signed as follows:

Signed By:	[redacted]
Date:	12/16/2019
Time:	04:50:14 AM (UTC)
Original Recipient:	[redacted]@gmail.com
IP:	1.6.15.235
Message Id	AEBE468BF42A52CD91F393CBC6E922E1EA26718C
Client Code	

RPost® Technologies: General terms, conditions, service levels, legal, trademark, and patent notices are available on RPost company (www.rmail.com) and product websites (https://www.rmail.com/legal-notices-2/legal-patent-notice/) RPost's services, including RMail®, RSign®, Registered Email™, SideNote®, RMail encryption, and others are RPost patented technologies protected with US and non-US patent applications and US patents 8209389, 8224913, 8468199, 8161104, 8468198, 8504628, 7966372, 6182219, 6571334, 8484706, 9100355, 7707624, and other US and non-US patents listed at RPost company (www.rmail.com) and product websites (https://www.rpost.com/about-rpost/intellectual-property/trademarks).

RPost ® Patented

Figure 3.1.19: RPost eSignOff Service email

TASK 1.8

View Acknowledgement Emails as a Sender

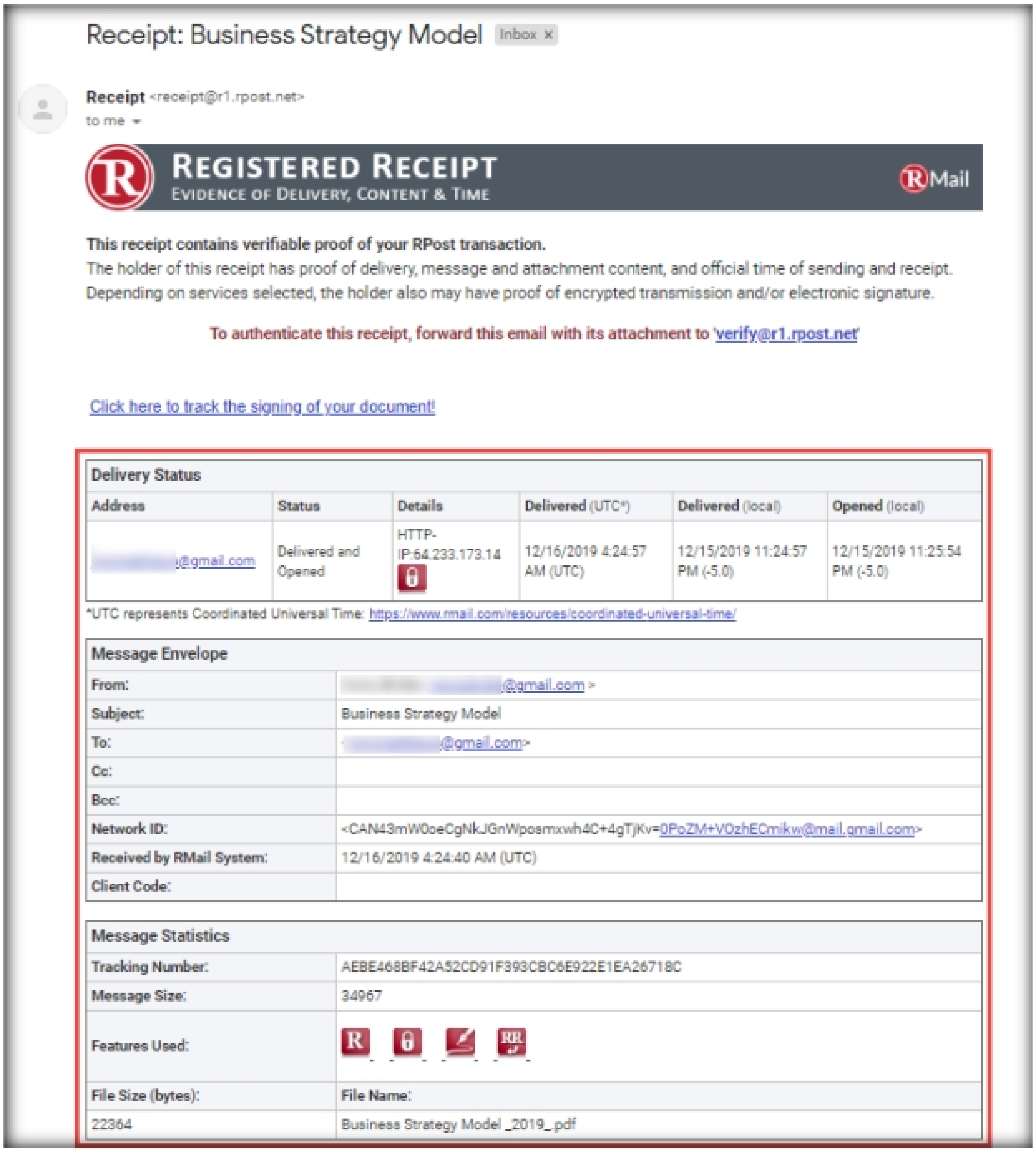
35. Now, return to the **Windows 10** virtual machine, where the sender's account is opened. In **Inbox**, you can observe two emails (**Receipt** and **RPost eSignOff Service**). Click to open the **Receipt** email.

Note: You might receive a **Receipt** mail in the **RMail Receipts** inbox folder present in the left-hand pane.

36. The **Receipt** email contains information about the **Delivery Status**, **Message Envelope**, and **Message Statistics** of the sent email, as shown in the screenshot.

37. The **Receipt** email also includes the **DeliveryReceipt** and **HtmlReceipt** attachments containing detailed information regarding the sent email.

You can also use other email encryption tools such as **Virtru** (https://www.virtru.com), **ZixMail** (https://www.zixcorp.com), **Egress Secure Email and File Transfer** (https://www.egress.com), and **Proofpoint Email Protection** (https://www.proofpoint.com) to perform email encryption.



Receipt: Business Strategy Model

Receipt <receipt@r1.rpost.net>
to me

This receipt contains verifiable proof of your RPost transaction.
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net'

Click here to track the signing of your document!

Delivery Status

Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
[redacted]@gmail.com	Delivered and Opened	HTTP-IP:64.233.173.14	12/16/2019 4:24:57 AM (UTC)	12/15/2019 11:24:57 PM (-5.0)	12/15/2019 11:25:54 PM (-5.0)

*UTC represents Coordinated Universal Time: https://www.rmail.com/resources/coordinated-universal-time/

Message Envelope

From:	[redacted]@gmail.com >
Subject:	Business Strategy Model
To:	<[redacted]@gmail.com>
Cc:	
Bcc:	
Network ID:	<CAN43mW0oeCgNkJGnWposmxwh4C+4gTjKv=0PoZM+VOzhECmikw@mail.gmail.com>
Received by RMail System:	12/16/2019 4:24:40 AM (UTC)
Client Code:	

Message Statistics

Tracking Number:	AEBE468BF42A52CD91F393CBC6E922E1EA26718C
Message Size:	34967
Features Used:	R RR
File Size (bytes):	File Name:
22364	Business Strategy Model _2019_.pdf

Figure 3.1.20: Receipt email

38. Now, navigate back to the **Inbox** and open an email from **RPost eSignOff Service**. This email contains the same information as the email received from **RPost eSignOff Service** by the recipient.

39. This concludes the demonstration of performing email encryption using RMail.
40. Close all open windows and document all the acquired information.
41. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab 4

Perform Disk Encryption

Disk encryption encrypts every bit and byte of data stored on a disk or a disk volume, thus preventing illegal access to data storage.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography

Lab Objectives

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection

- VeraCrypt located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt**
- Rohos Disk Encryption located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 30 Minutes

Overview of Disk Encryption

Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

Lab Tasks

TASK 1

Perform Disk Encryption using VeraCrypt

Here, we will use the VeraCrypt tool to perform disk encryption.

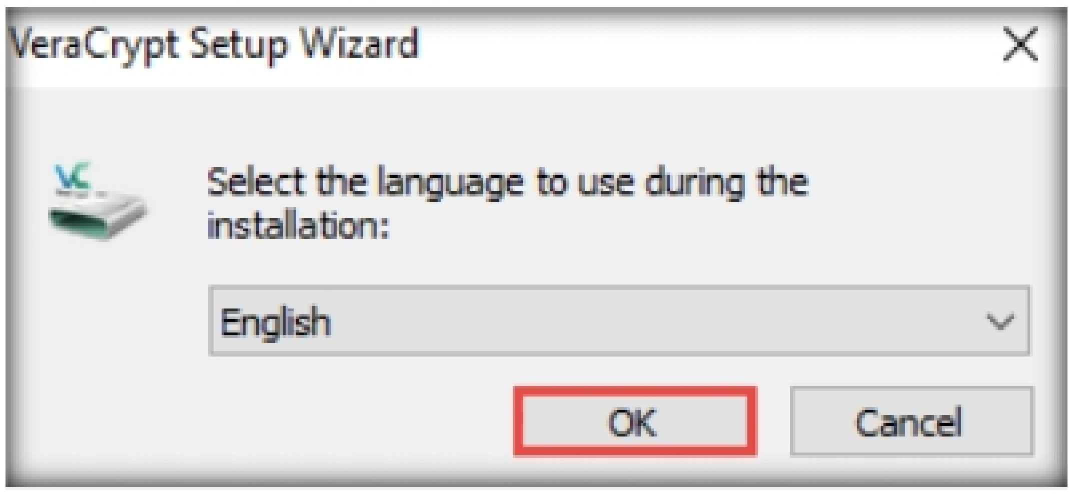
TASK 1.1

Install and Launch VeraCrypt

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\VeraCrypt** and double-click **VeraCrypt Setup 1.24-Hotfix1.exe**.

Note: If the **User Account Control** pop-up appears, click **Yes**.

3. **VeraCrypt Setup Wizard** appears, click **OK**.



VeraCrypt Setup Wizard

Select the language to use during the installation:

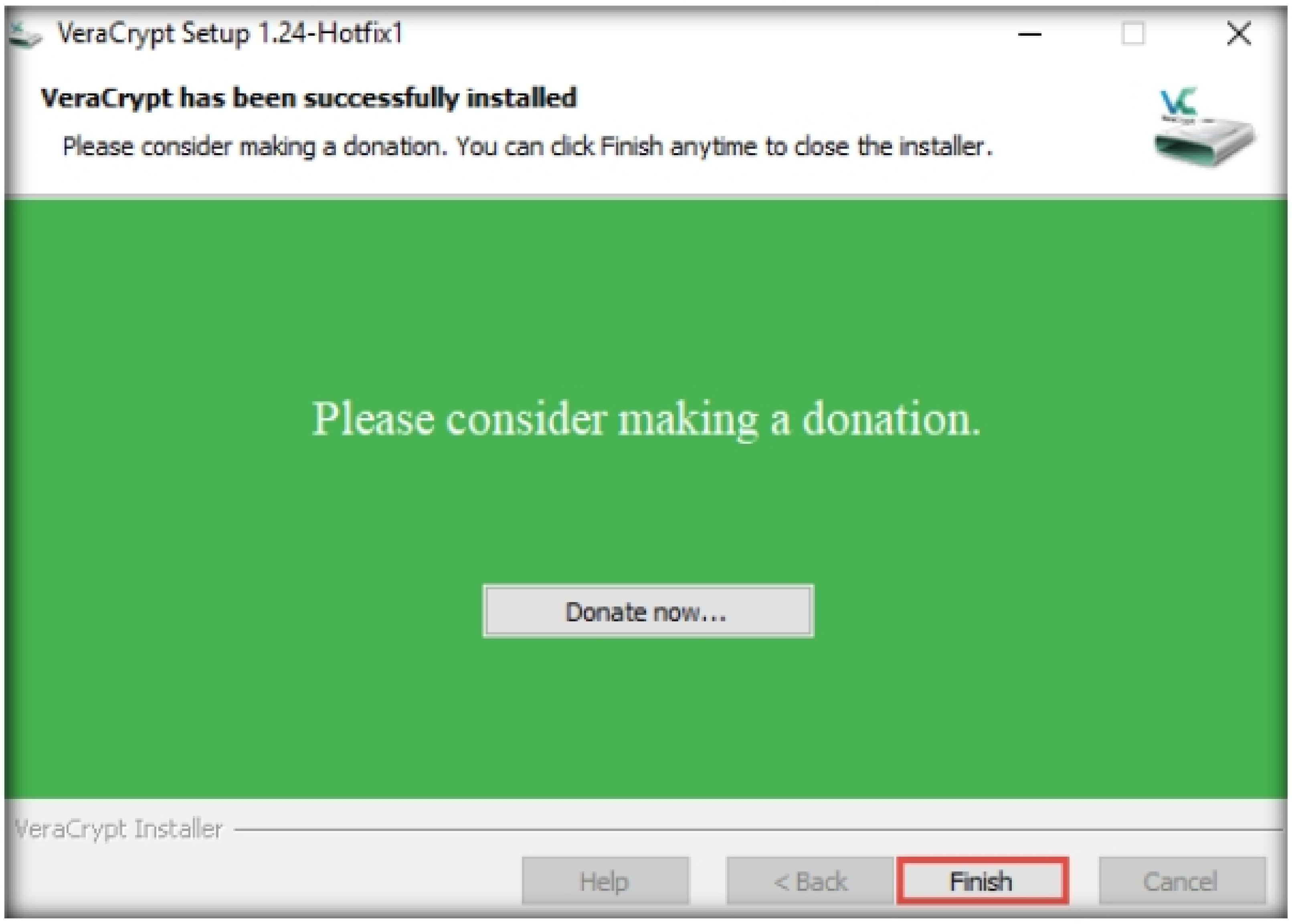
English

Figure 4.1.1: VeraCrypt Setup Wizard

4. Follow the steps to install the application using all default settings.

VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

5. After the completion of the installation, the **VeraCrypt has been successfully installed** wizard appears; then, click **Finish**.



VeraCrypt Setup 1.24-Hotfix1

VeraCrypt has been successfully installed

Please consider making a donation. You can click Finish anytime to close the installer.

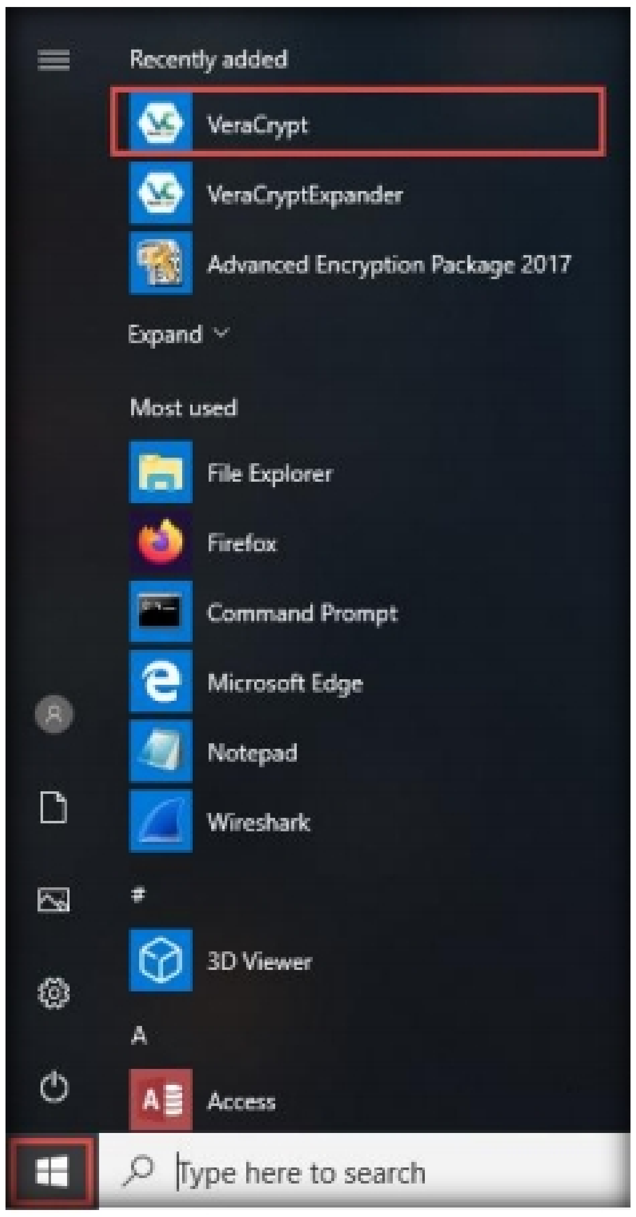
Please consider making a donation.

Donate now...
VeraCrypt Installer
Help
< Back
Finish
Cancel

Figure 4.1.2: VeraCrypt has been successfully installed wizard

6. A **VeraCrypt Setup** notification appears; then, click **No**.

7. Click the **Start** icon in the bottom-left corner of **Desktop** and click **VeraCrypt** from the applications to launch VeraCrypt.



Recently added
VeraCrypt
VeraCryptExpander
Advanced Encryption Package 2017
Expand
Most used
File Explorer
Firefox
Command Prompt
Microsoft Edge
Notepad
Wireshark
#
3D Viewer
A
Access
Type here to search

Figure 4.1.3: Launch VeraCrypt

TASK 1.2

Create a Volume

8. The **VeraCrypt** main window appears; click the **Create Volume** button.

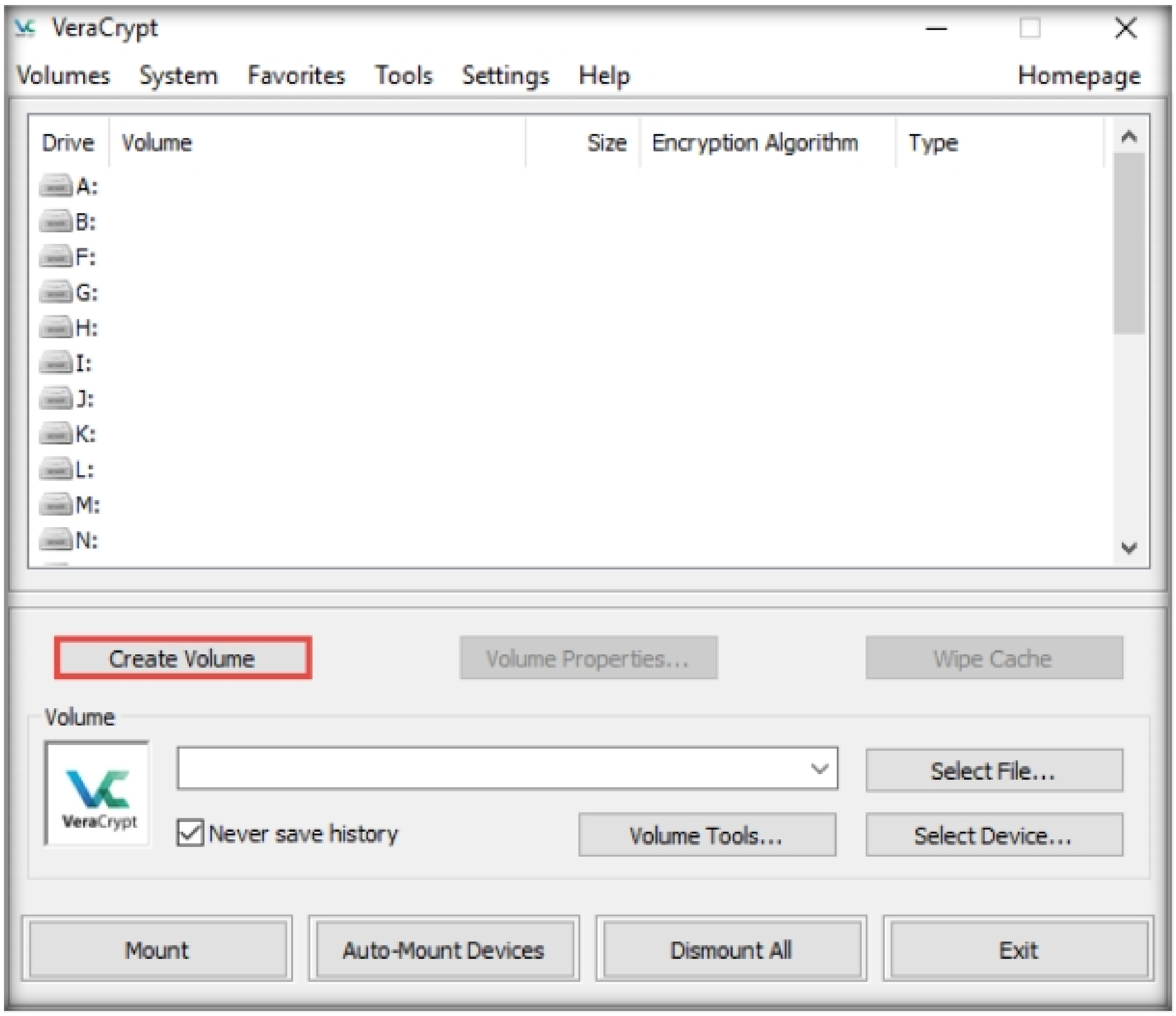
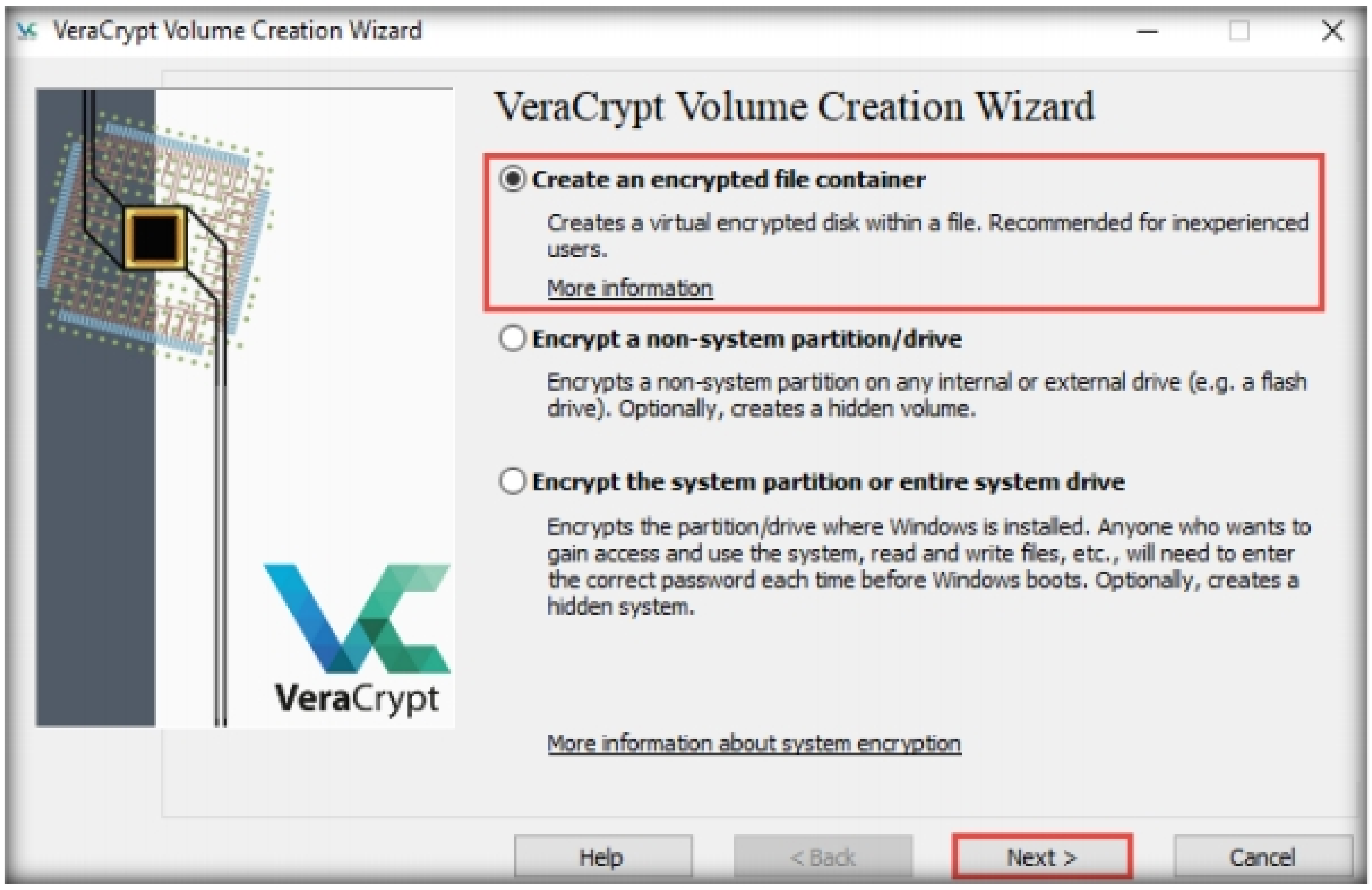

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Create Volume
Volume Properties...
Wipe Cache
Volume
VeraCrypt
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Figure 4.1.4: VeraCrypt main window

9. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.


VeraCrypt Volume Creation Wizard

● **Create an encrypted file container**

Creates a virtual encrypted disk within a file. Recommended for inexperienced users.

More information

○ **Encrypt a non-system partition/drive**

Encrypts a non-system partition on any internal or external drive (e.g. a flash drive). Optionally, creates a hidden volume.

○ **Encrypt the system partition or entire system drive**

Encrypts the partition/drive where Windows is installed. Anyone who wants to gain access and use the system, read and write files, etc., will need to enter the correct password each time before Windows boots. Optionally, creates a hidden system.

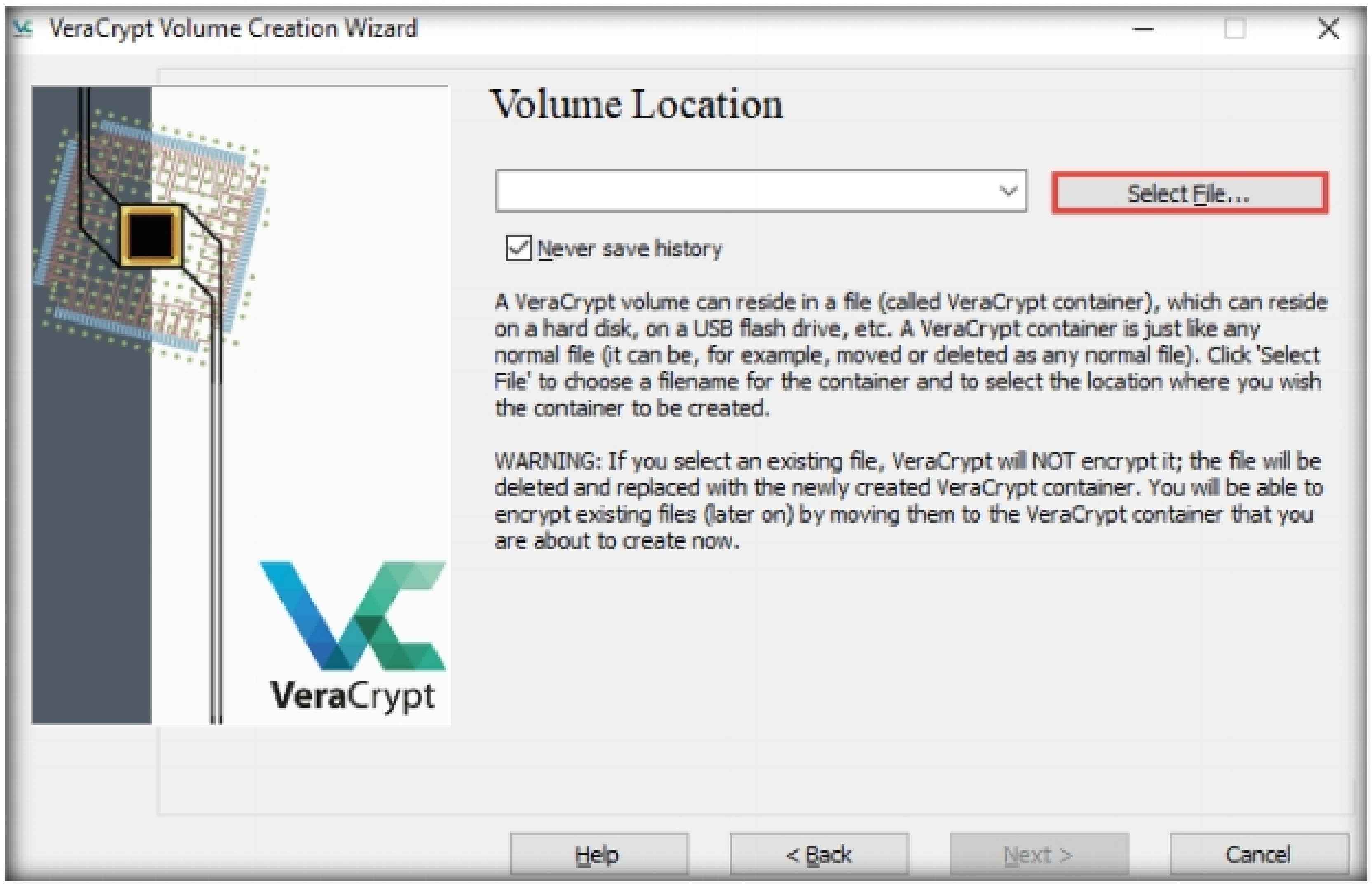
More information about system encryption

VeraCrypt Volume Creation Wizard
VeraCrypt
Help
< Back
Next >
Cancel

Figure 4.1.5: VeraCrypt Volume Creation Wizard

10. In the **Volume Type** wizard, keep the default settings and click **Next**.

11. In the **Volume Location** wizard, click **Select File...**.



VeraCrypt Volume Creation Wizard
Volume Location
Select File...
Help
< Back
Next >
Cancel
VeraCrypt

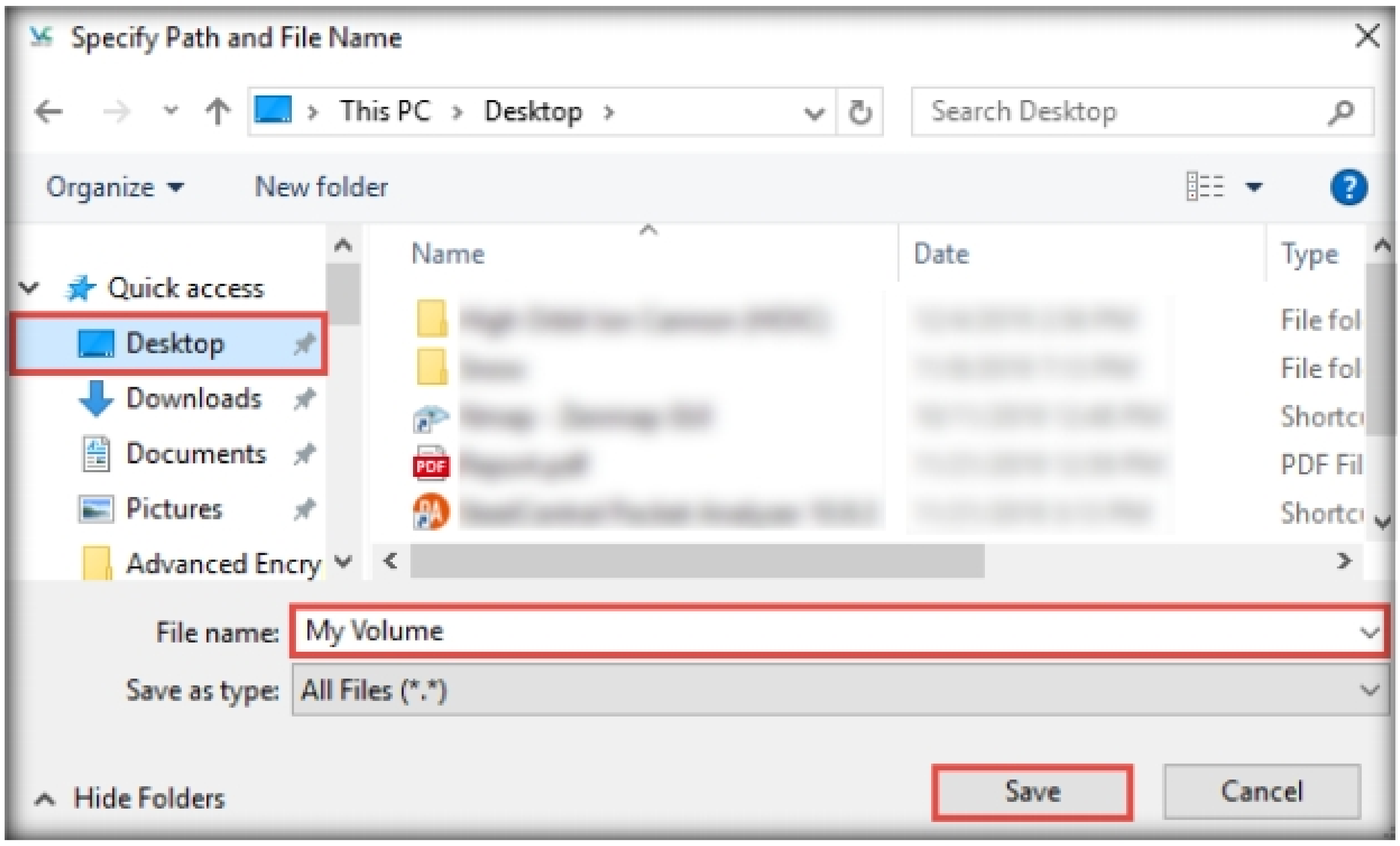
☑ Never save history

A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

Figure 4.1.6: VeraCrypt Volume Creation Wizard-Volume Location

12. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **My Volume**, and click **Save**.



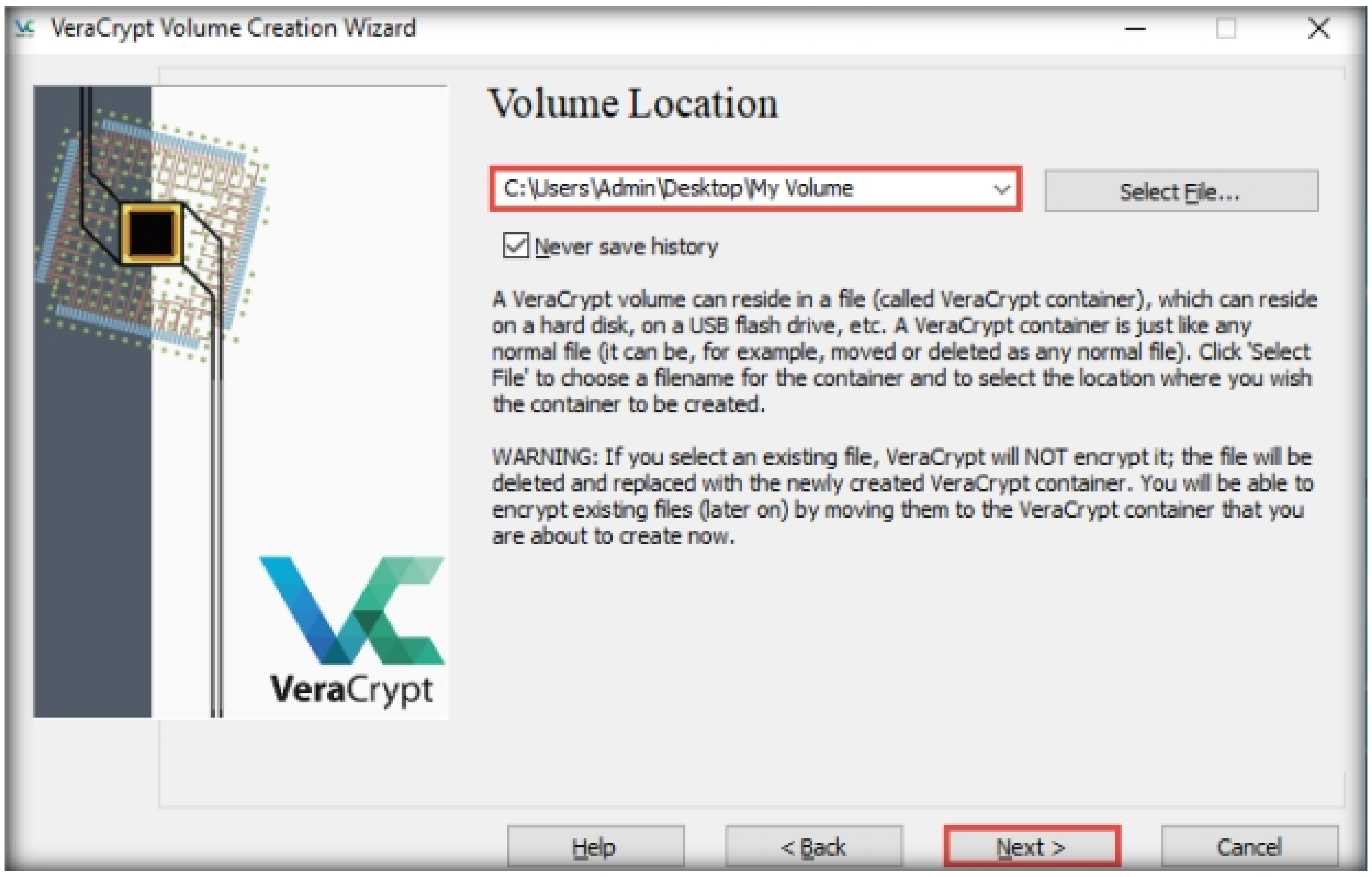
Specify Path and File Name
This PC > Desktop >
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Advanced Ency
Name
Date
Type
File fol
File fol
Shortc
PDF Fil
Shortc
Save
Cancel
Hide Folders

File name: My Volume

Save as type: All Files (*.*)

Figure 4.1.7: Specify Path and File Name Window

13. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.



Volume Location

C:\Users\Admin\Desktop\My Volume

☑ Never save history

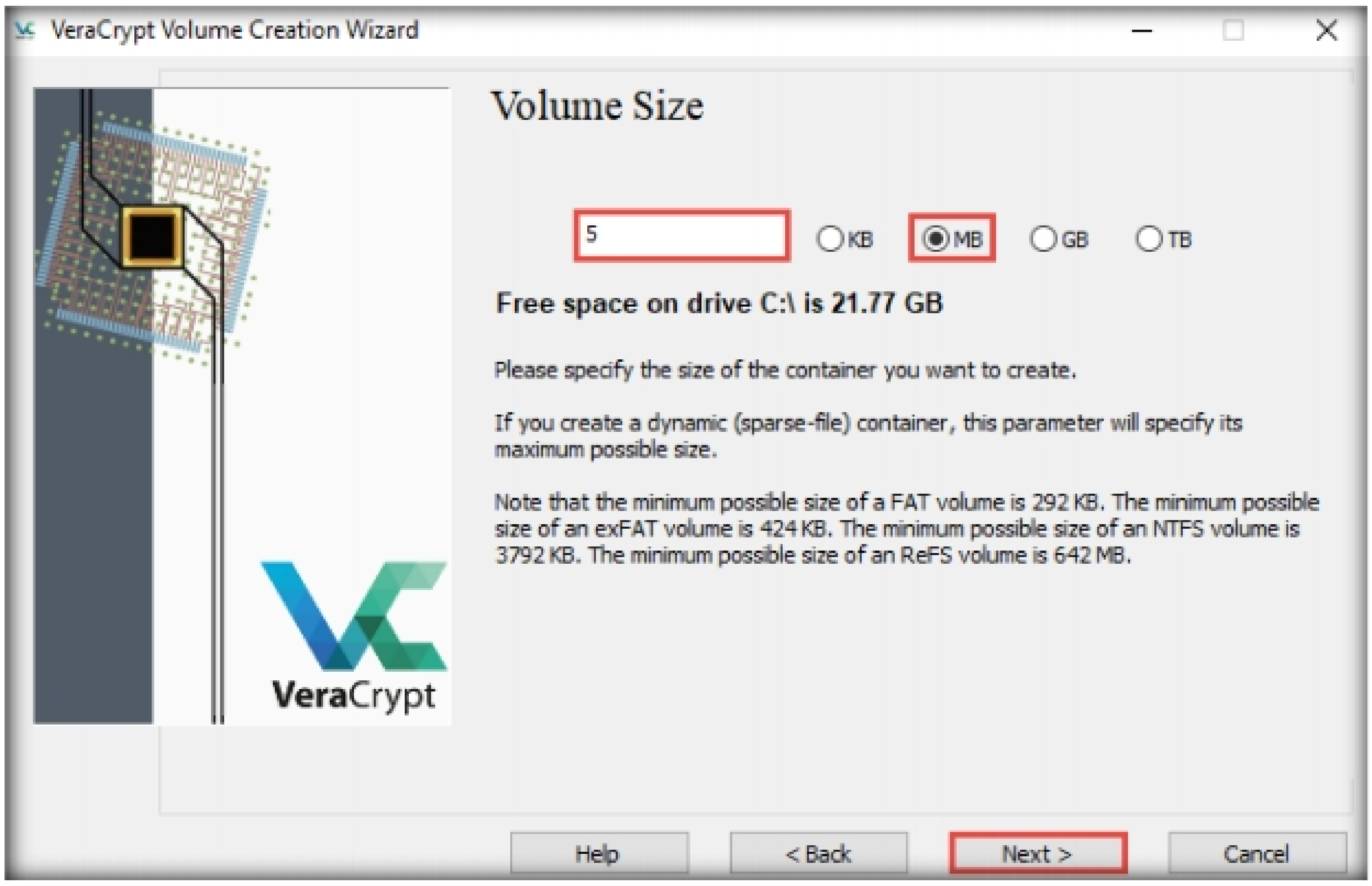
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.

WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.

Figure 4.1.8: VeraCrypt Volume Creation Wizard: Volume Location

14. In the **Encryption Options** wizard, keep the default settings and click **Next**.

15. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.



Volume Size

5 ○ KB ● MB ○ GB ○ TB

Free space on drive C:\ is 21.77 GB

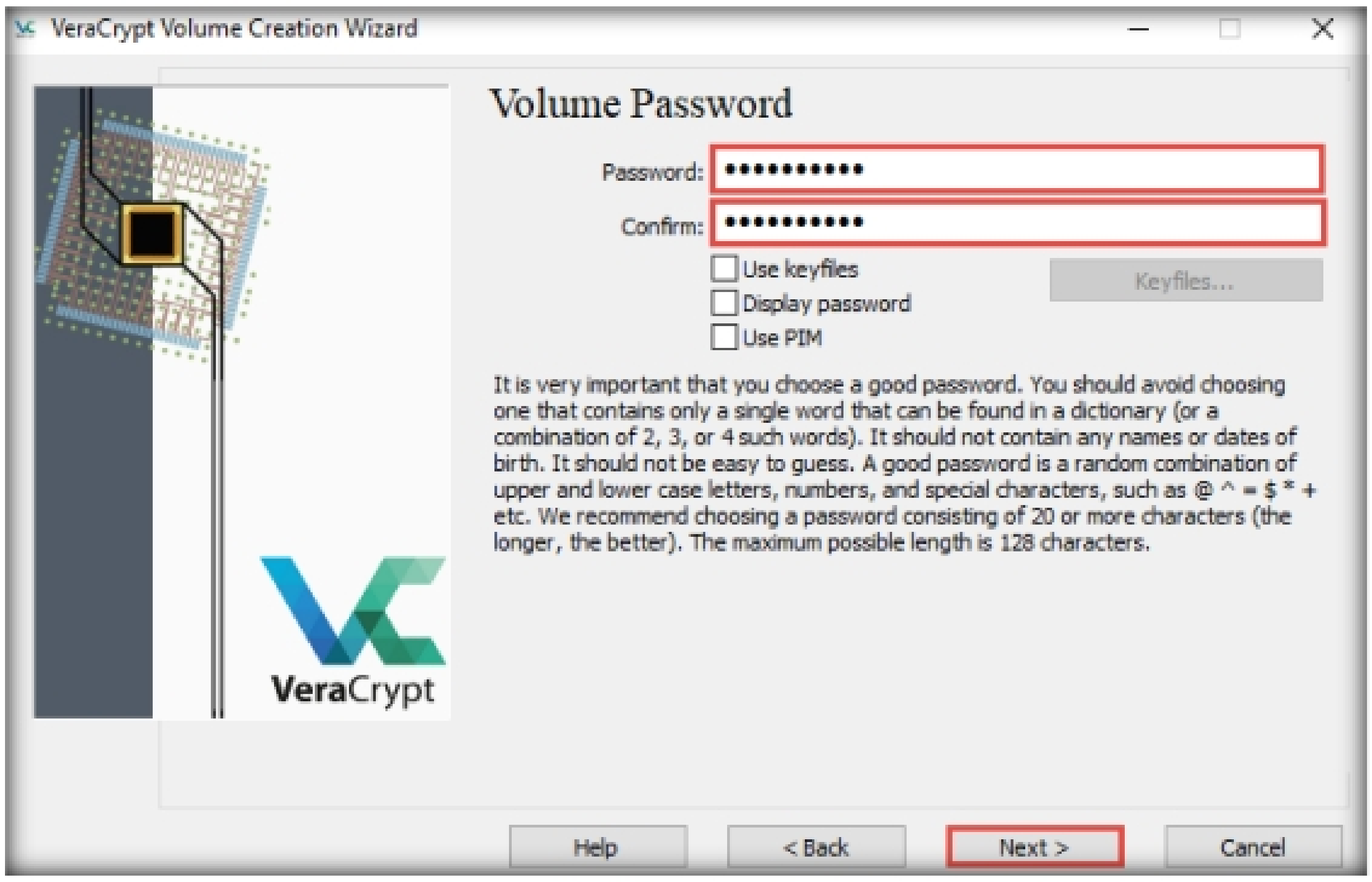
Please specify the size of the container you want to create.

If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.

Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an exFAT volume is 424 KB. The minimum possible size of an NTFS volume is 3792 KB. The minimum possible size of an ReFS volume is 642 MB.

Figure 4.1.9: VeraCrypt Volume Creation Wizard-Volume Size

16. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.


VeraCrypt Volume Creation Wizard
Keyfiles...
VeraCrypt
Help
< Back
Next >
Cancel

Volume Password

Password: ••••••••••

Confirm: ••••••••••

☐ Use keyfiles
☐ Display password
☐ Use PIM

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 128 characters.

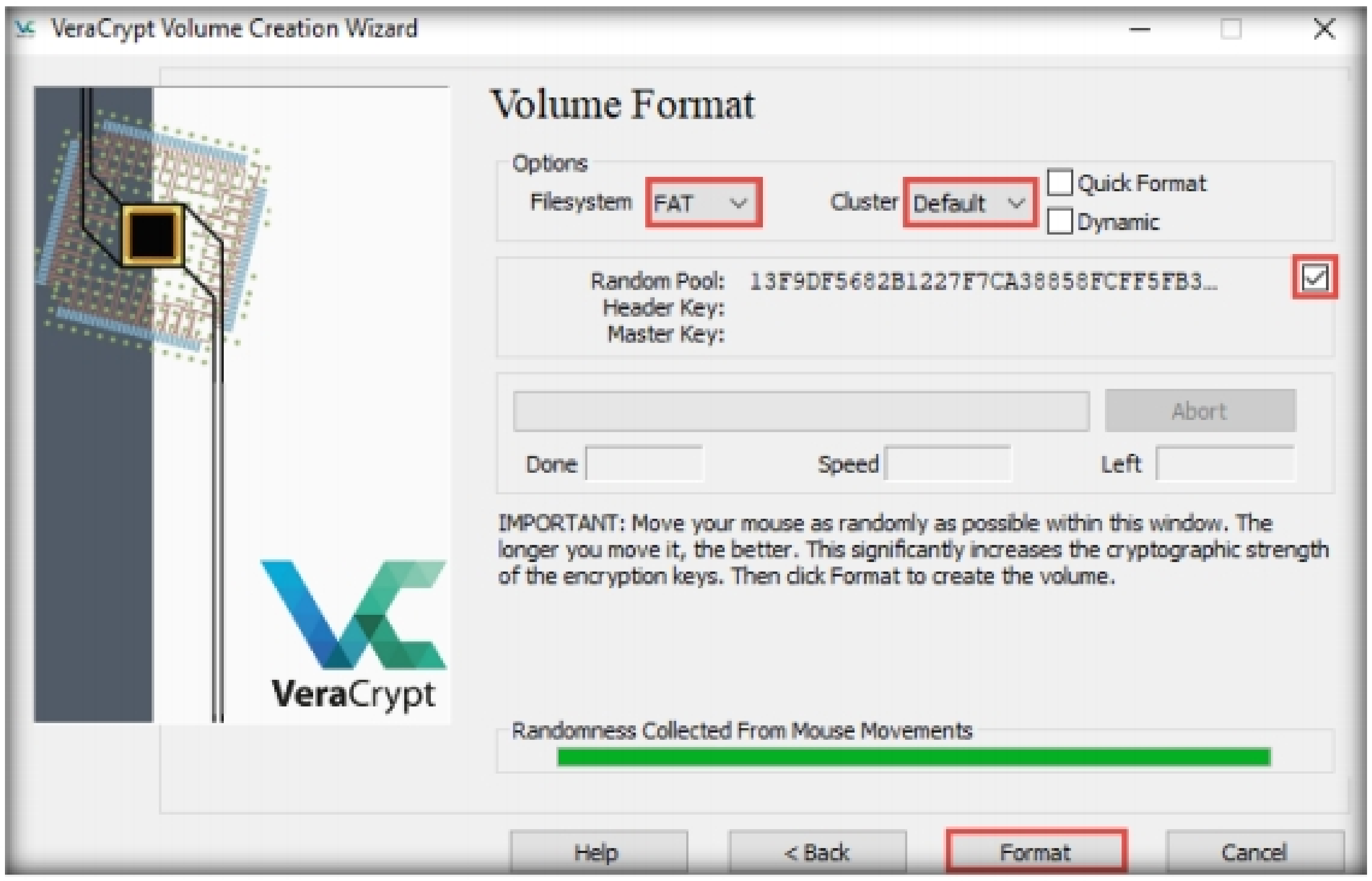
Figure 4.1.10: VeraCrypt Volume Creation Wizard: Volume Password

Note: A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

17. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.

18. Check the checkbox under the **Random Pool**, **Header Key**, and **Master Key** section.

19. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.


VeraCrypt Volume Creation Wizard
Abort
Done
Speed
Left
VeraCrypt
Randomness Collected From Mouse Movements
Help
< Back
Format
Cancel

Volume Format

Options

Filesystem FAT

Cluster Default

☐ Quick Format
☐ Dynamic

Random Pool: 13F9DF5682B1227F7CA38858FCFF5FB3... ☑

Header Key:

Master Key:

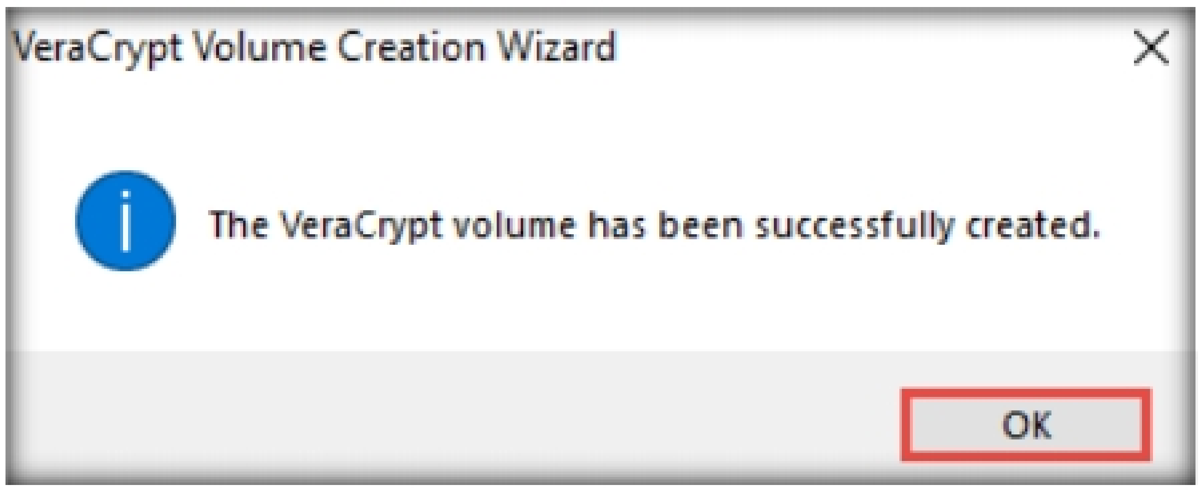
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.

Figure 4.1.11: VeraCrypt Volume Creation Wizard-Volume Format

20. After clicking **Format**, VeraCrypt will create a file called **My Volume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).

21. Depending on the size of the volume, volume creation may take some time.

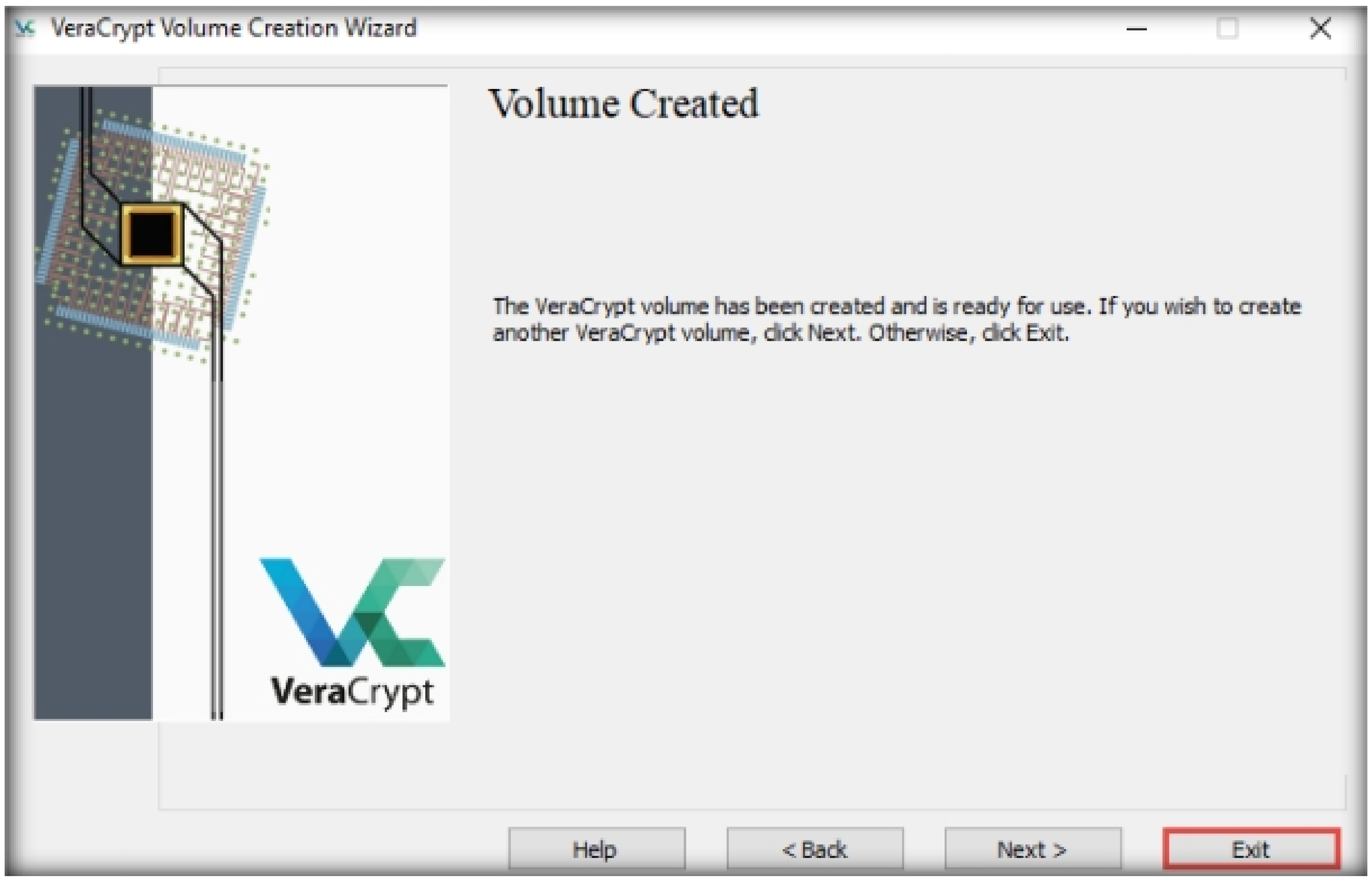
22. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.


VeraCrypt Volume Creation Wizard
OK

The VeraCrypt volume has been successfully created.

Figure 4.1.12: VeraCrypt Volume Creation Wizard Dialog Box

23. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.


VeraCrypt Volume Creation Wizard
Volume Created
VeraCrypt
Help
< Back
Next >
Exit

The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.

Figure 4.1.13: VeraCrypt Volume Creation Wizard-Volume Created

TASK 1.3

Mount a Volume

24. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File...**.

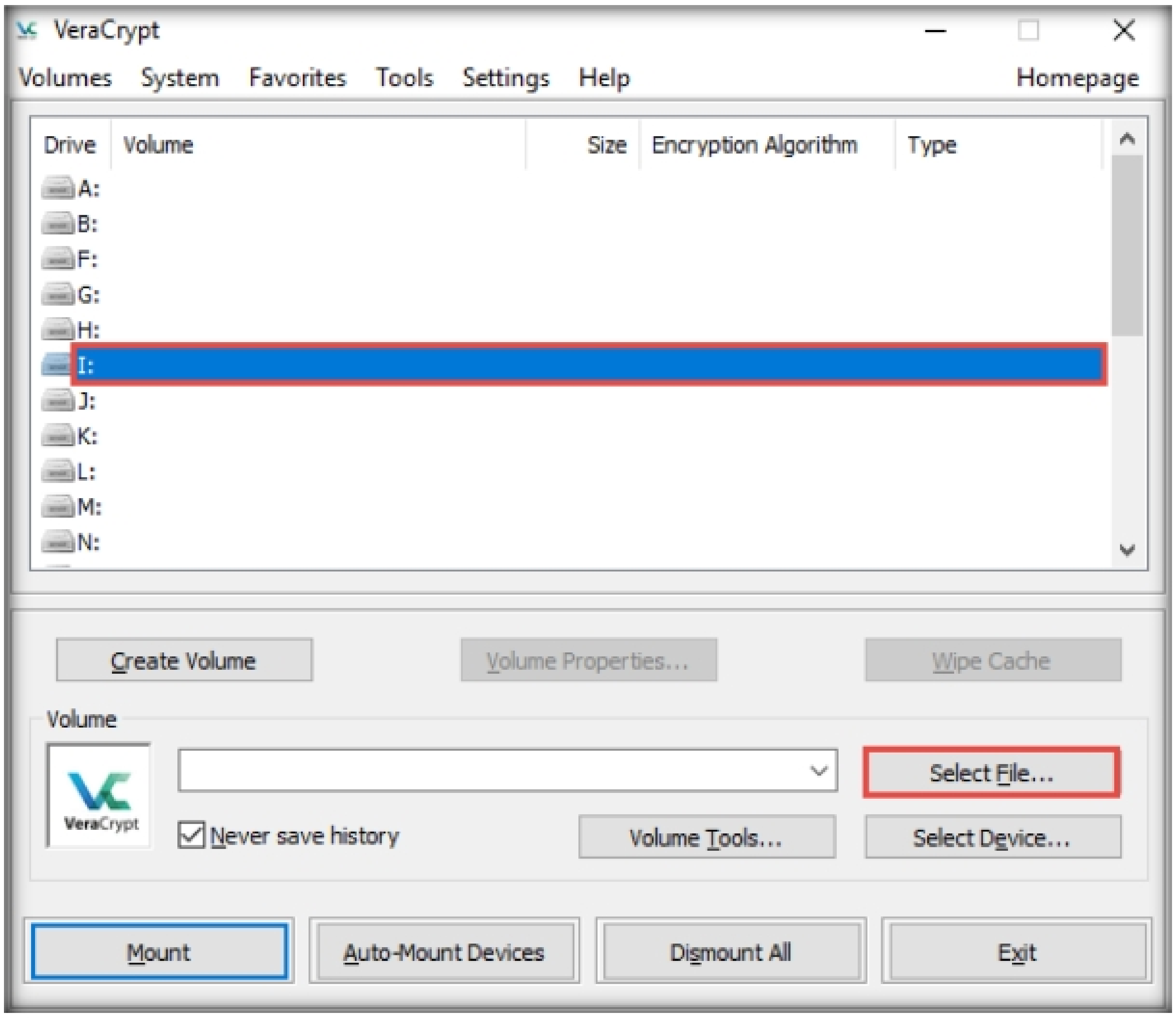

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Create Volume
Volume Properties...
Wipe Cache
Volume
VeraCrypt
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Figure 4.1.14: VeraCrypt Main Window with Select File Button

25. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **My Volume**, and click **Open**.

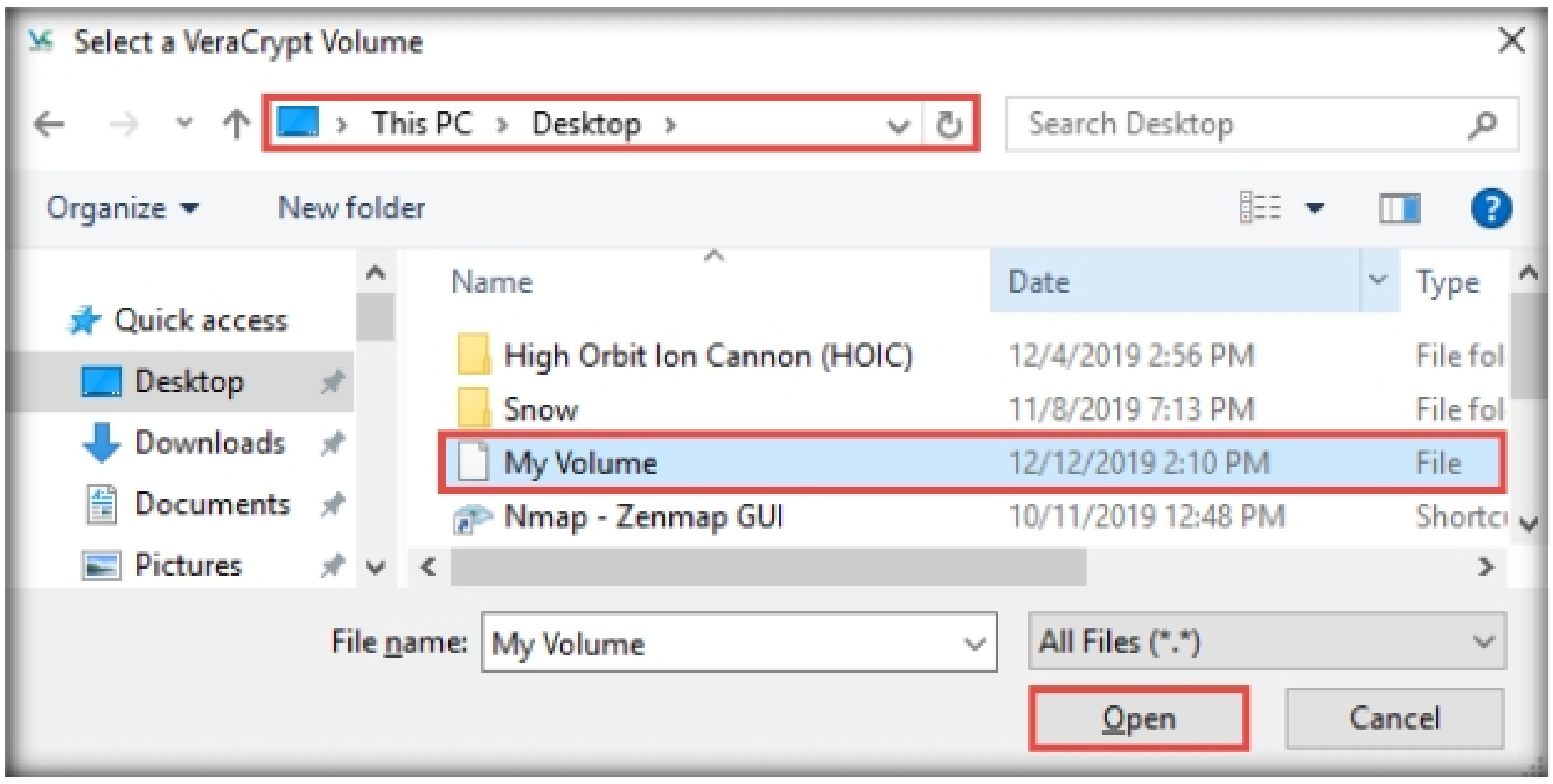
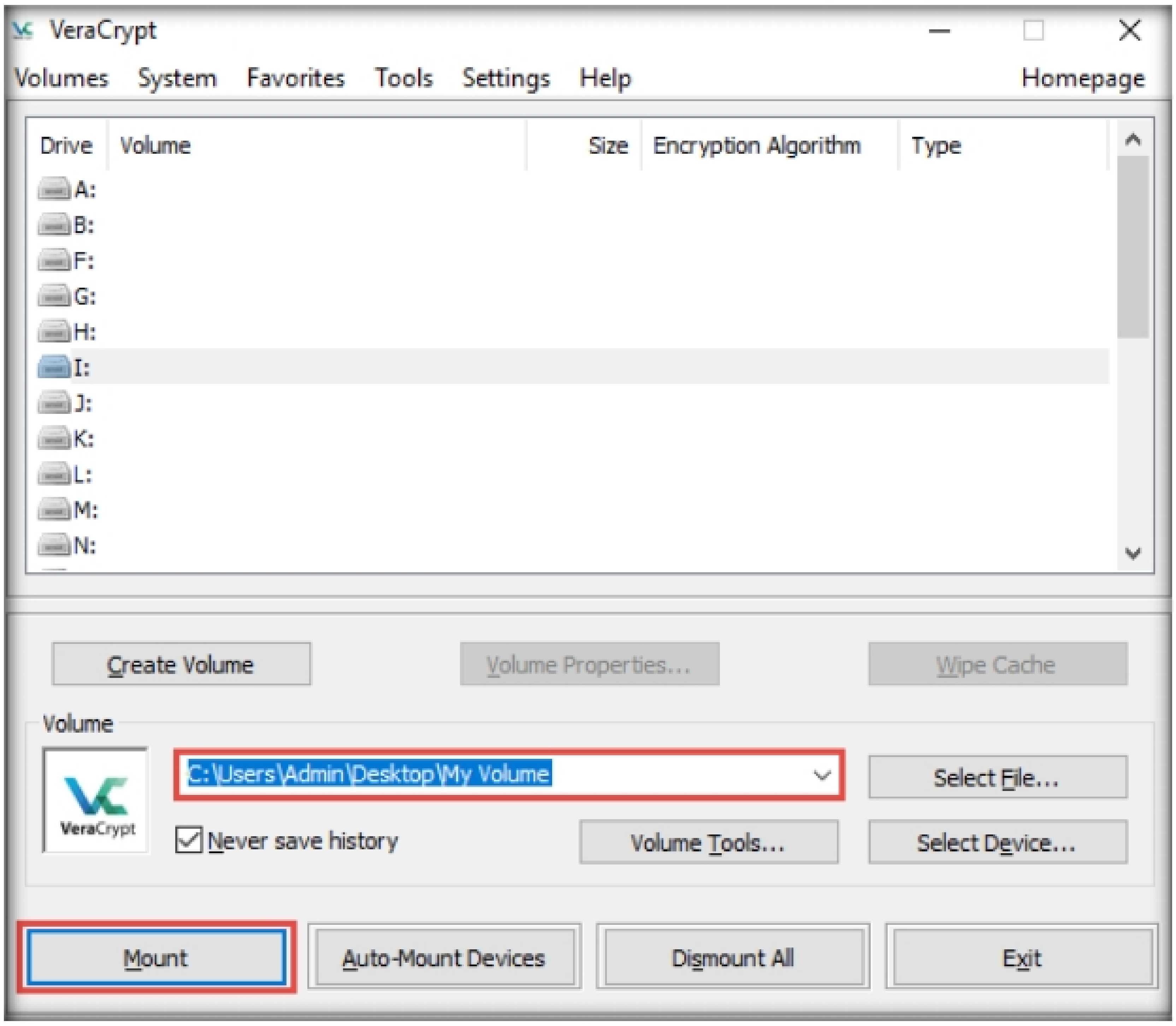

Select a VeraCrypt Volume
This PC > Desktop >
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Name
Date
Type
High Orbit Ion Cannon (HOIC) 12/4/2019 2:56 PM File fol
Snow 11/8/2019 7:13 PM File fol
My Volume 12/12/2019 2:10 PM File
Nmap - Zenmap GUI 10/11/2019 12:48 PM Shortc
File name: My Volume
All Files (*.*)
Open
Cancel

Figure 4.1.15: Windows Standard File Selector Window

26. The window closes, and the **VeraCrypt** window appears displaying the location of selected volume under the **Volume** field; then, click **Mount**.


VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
F:
G:
H:
I:
J:
K:
L:
M:
N:
Create Volume
Volume Properties...
Wipe Cache
Volume
VeraCrypt
Select File...
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

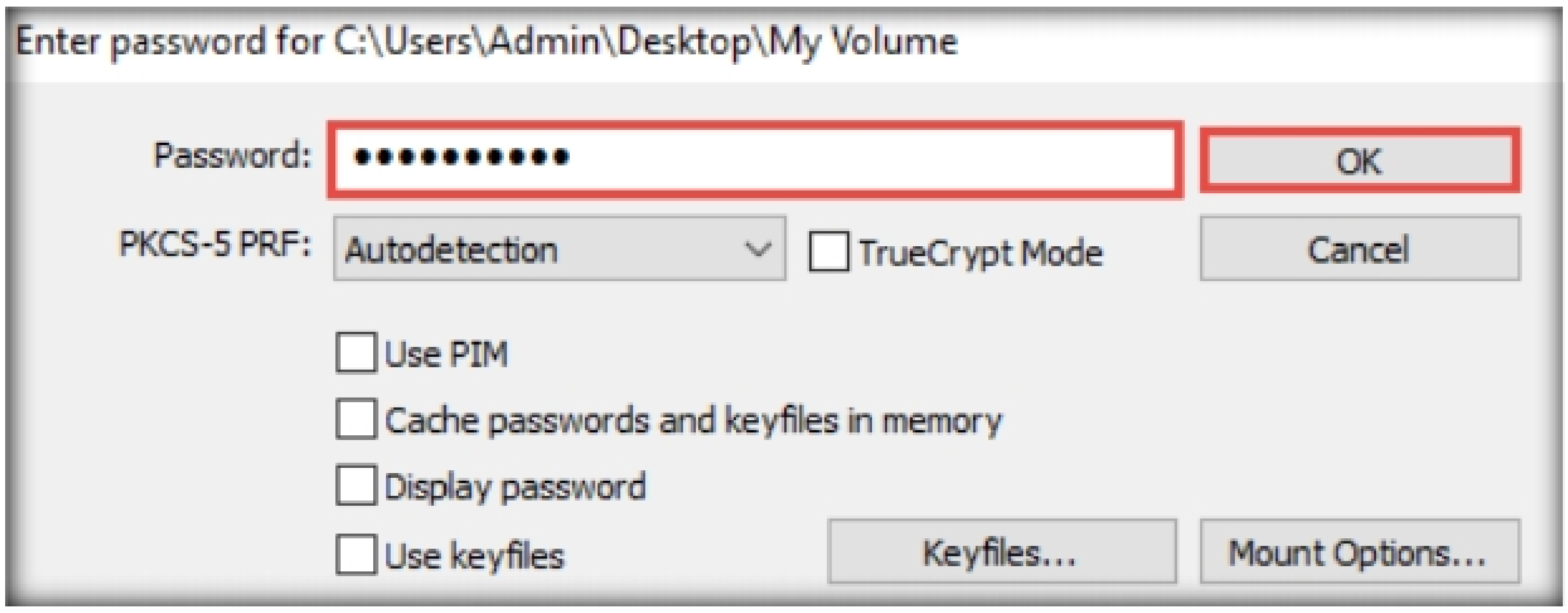
Volume: C:\Users\Admin\Desktop\My Volume

☑ Never save history

Figure 4.1.16: VeraCrypt Main Window with Mount Button

27. The **Enter password** dialog-box appears; type the password you specified in **Step#16** into the **Password** field and click **OK**.

Note: The password specified in this task is **qwerty@123**.


OK
Cancel
Keyfiles...
Mount Options...

Enter password for C:\Users\Admin\Desktop\My Volume

Password: ••••••••••

PKCS-5 PRF: Autodetection

☐ TrueCrypt Mode

☐ Use PIM

☐ Cache passwords and keyfiles in memory

☐ Display password

☐ Use keyfiles

Figure 4.1.17: VeraCrypt Enter password

28. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:

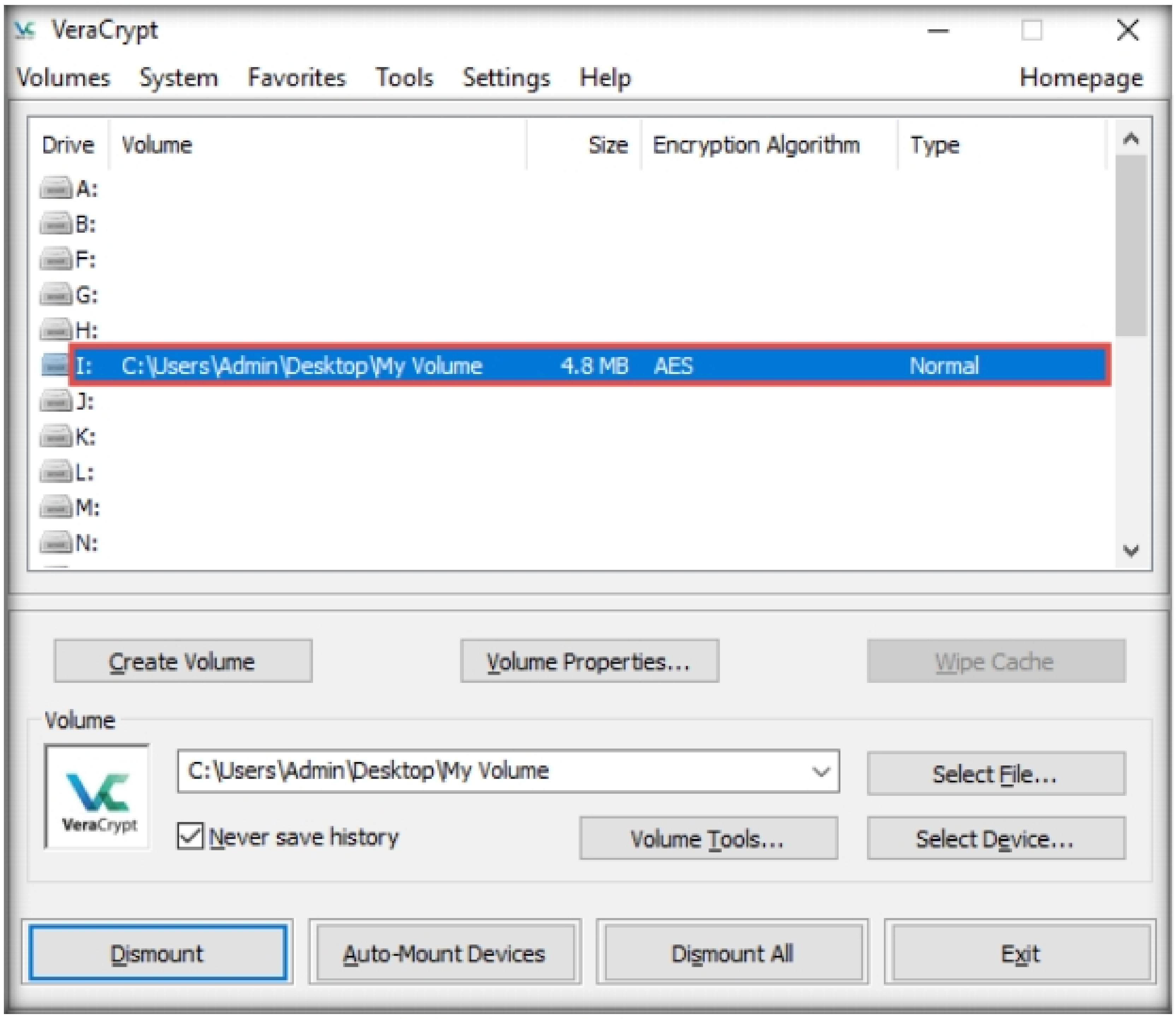

VeraCrypt
Volumes System Favorites Tools Settings Help Homepage
Drive Volume Size Encryption Algorithm Type
A:
B:
F:
G:
H:
I: C:\Users\Admin\Desktop\My Volume 4.8 MB AES Normal
J:
K:
L:
M:
N:
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\Admin\Desktop\My Volume
Select File...
☑ Never save history
Volume Tools...
Select Device...
Dismount
Auto-Mount Devices
Dismount All
Exit

Figure 4.1.18: VeraCrypt Main Window

29. **My Volume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

30. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

31. Click **File** in the menu bar and click **Save**.

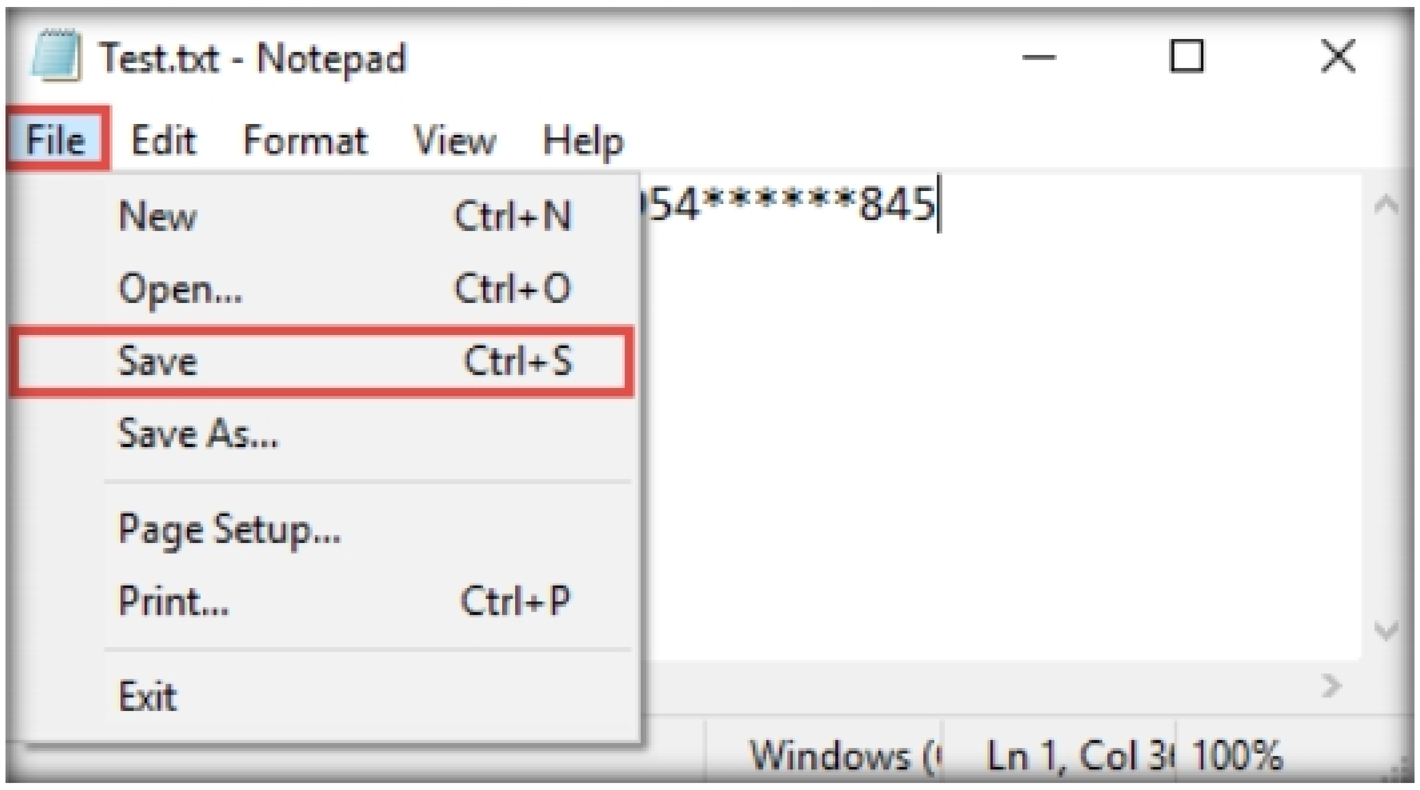

Test.txt - Notepad
File Edit Format View Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
54******845
Windows (
Ln 1, Col 3
100%

Figure 4.1.19: Text file

32. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.

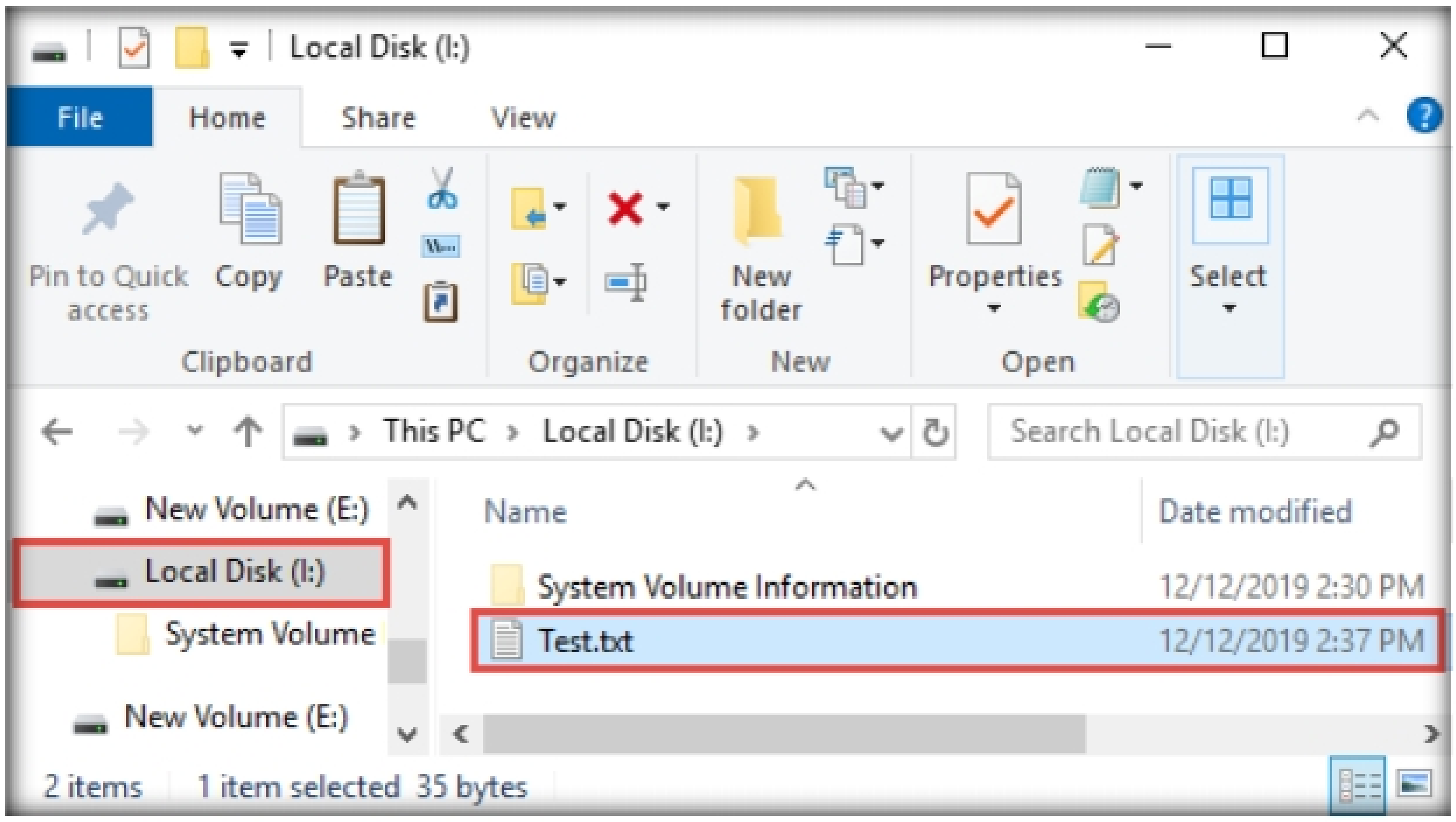

Local Disk (I:)
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Organize
New folder
New
Properties
Open
Select
This PC › Local Disk (I:) ›
Search Local Disk (I:)
New Volume (E:)
Local Disk (I:)
System Volume
New Volume (E:)
Name
Date modified
System Volume Information
12/12/2019 2:30 PM
Test.txt
12/12/2019 2:37 PM
2 items
1 item selected 35 bytes

Figure 4.1.20: Test.txt file in Encrypted Container

TASK 1.4

Dismount a Volume

33. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.

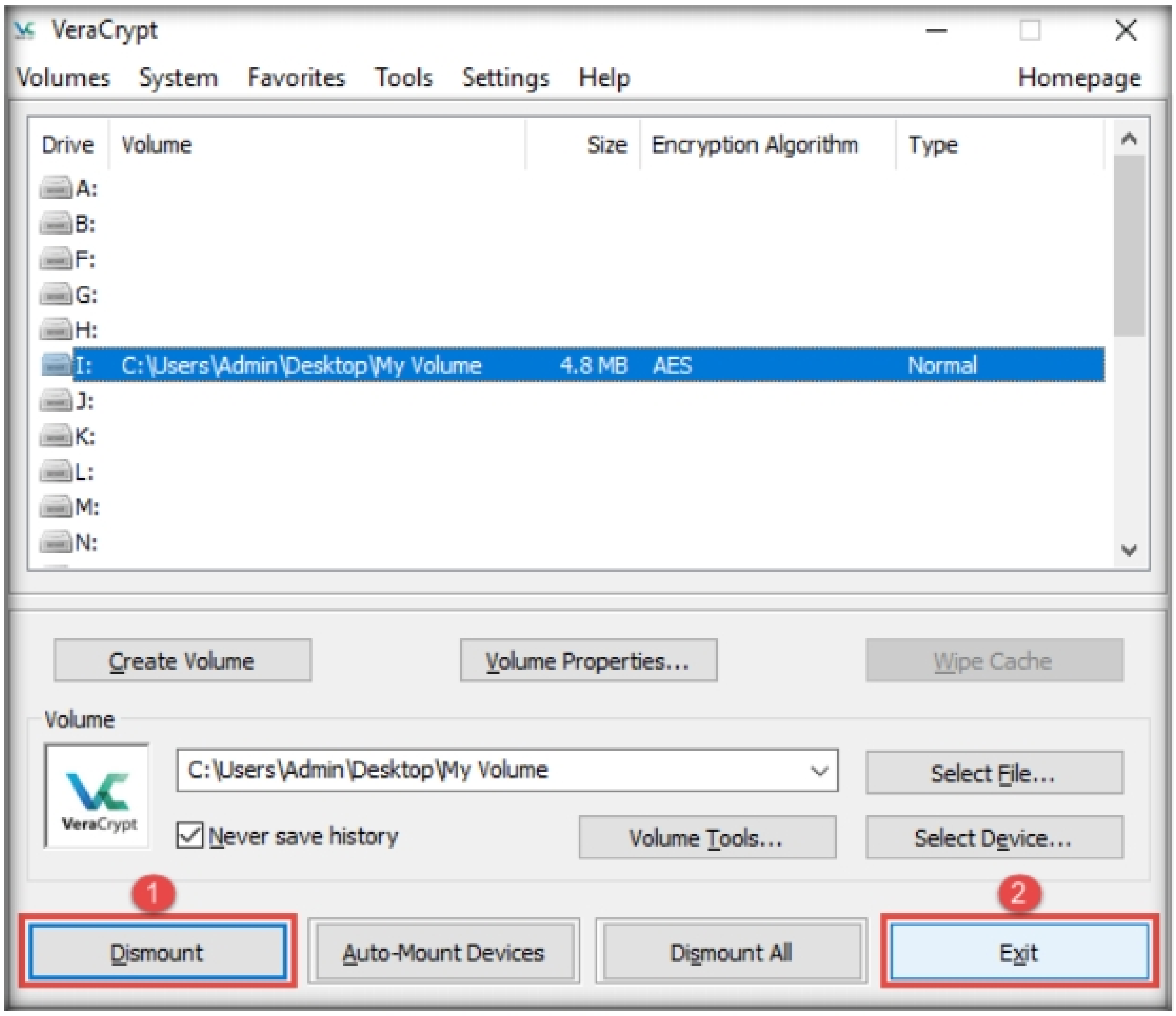

VeraCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption Algorithm
Type
A:
B:
F:
G:
H:
I: C:\Users\Admin\Desktop\My Volume 4.8 MB AES Normal
J:
K:
L:
M:
N:
Create Volume
Volume Properties...
Wipe Cache
Volume
C:\Users\Admin\Desktop\My Volume
Select File...
☑ Never save history
Volume Tools...
Select Device...
1
2
Dismount
Auto-Mount Devices
Dismount All
Exit

Figure 4.1.21: VeraCrypt Main Window with Dismount Button

34. The **I:** drive located in **This PC** disappears.

Note: This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume—including its files—unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

35. This concludes the demonstration of performing disk encryption using VeraCrypt.

36. Close all open windows and document all the acquired information.

TASK 2

Perform Disk Encryption using BitLocker Drive Encryption

Here, we will perform disk encryption using BitLocker Drive Encryption.

TASK 2.1

Launch BitLocker

1. In the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom-left corner of **Desktop** and type **bitlocker**. Select **Manage BitLocker** from the search results.

BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

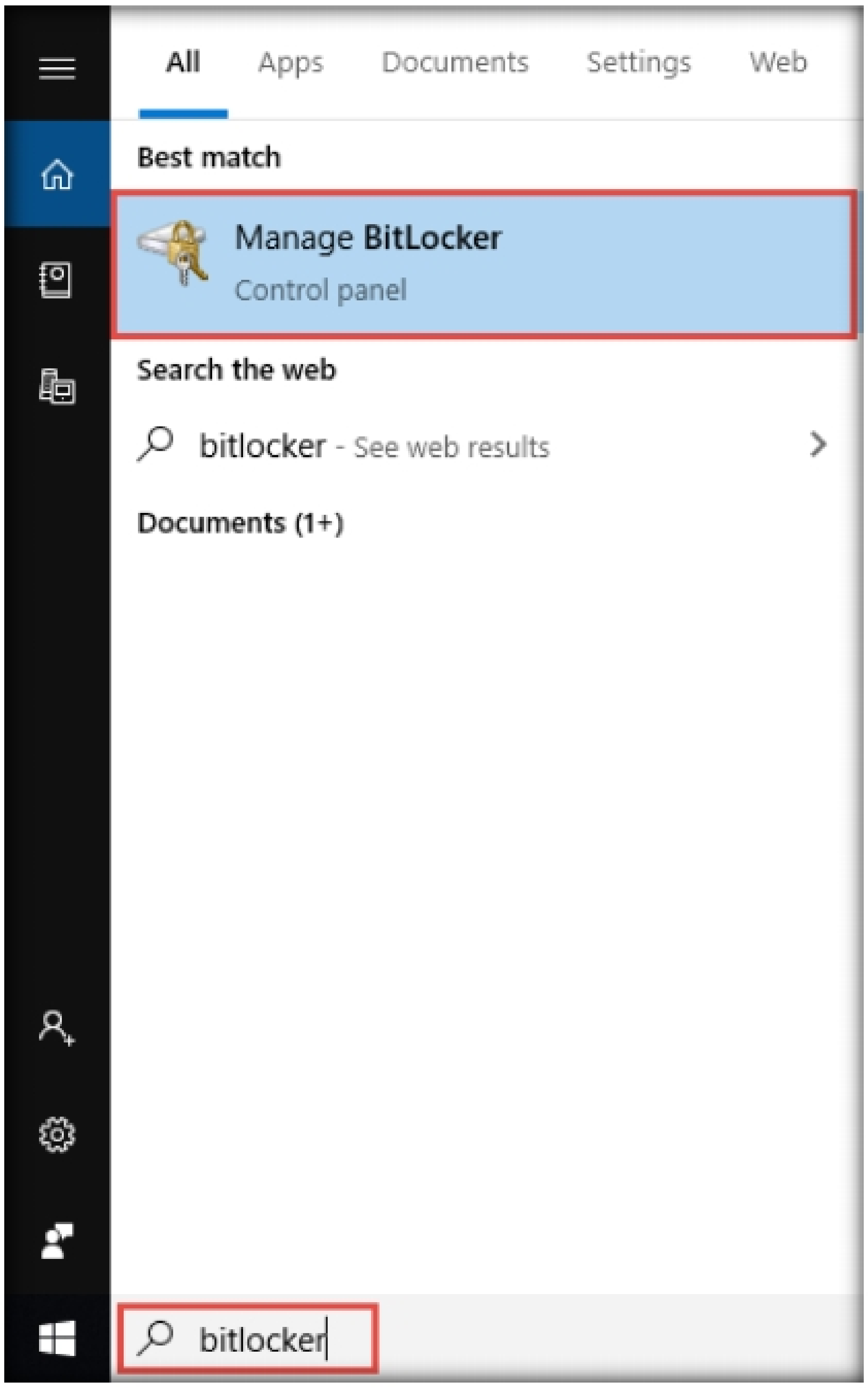
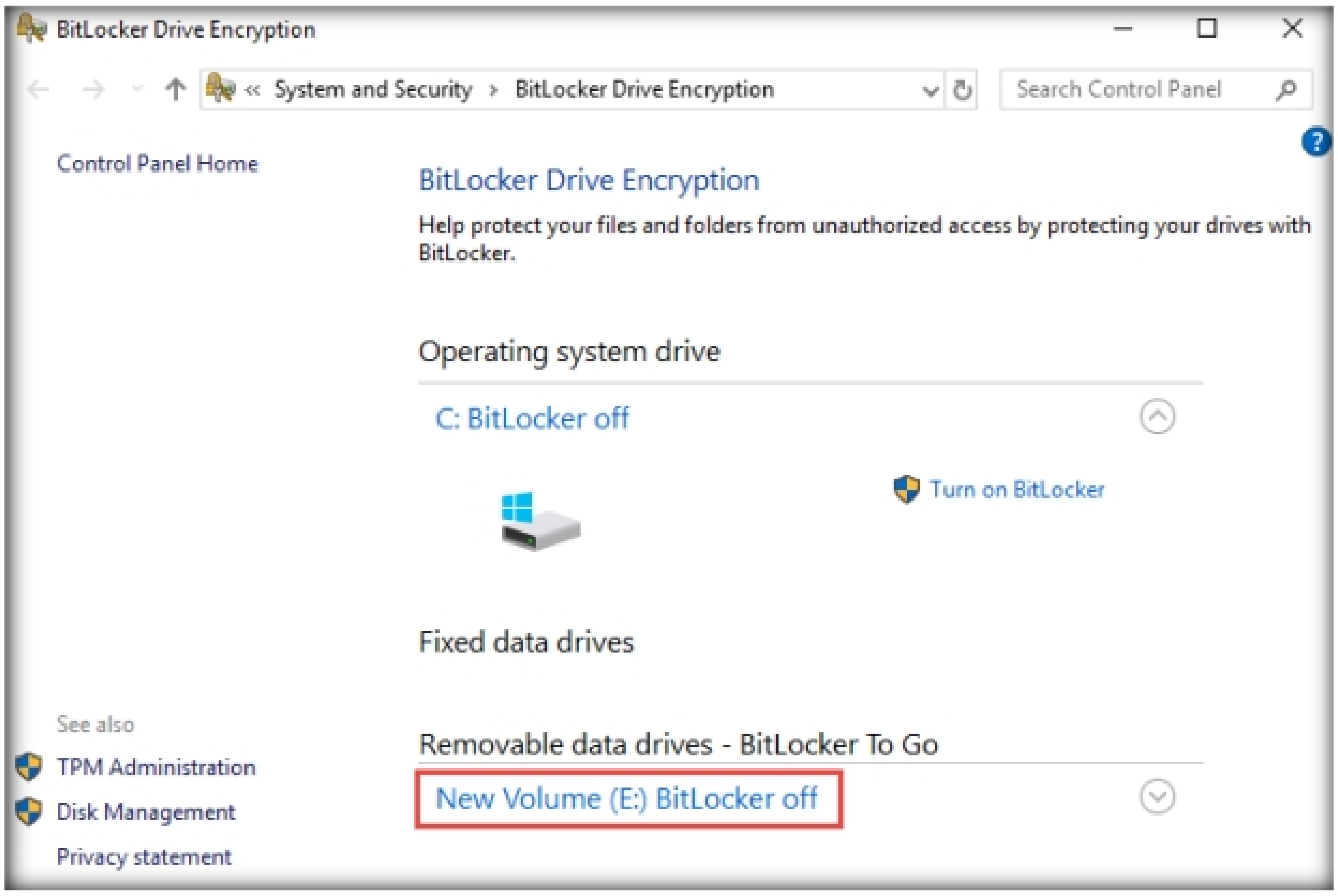


Figure 4.2.1: Launch BitLocker

2. The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Removable data drives - BitLocker To Go** section.


BitLocker Drive Encryption
« System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
Operating system drive
C: BitLocker off
Turn on BitLocker
Fixed data drives
Removable data drives - BitLocker To Go
New Volume (E:) BitLocker off
See also
TPM Administration
Disk Management
Privacy statement

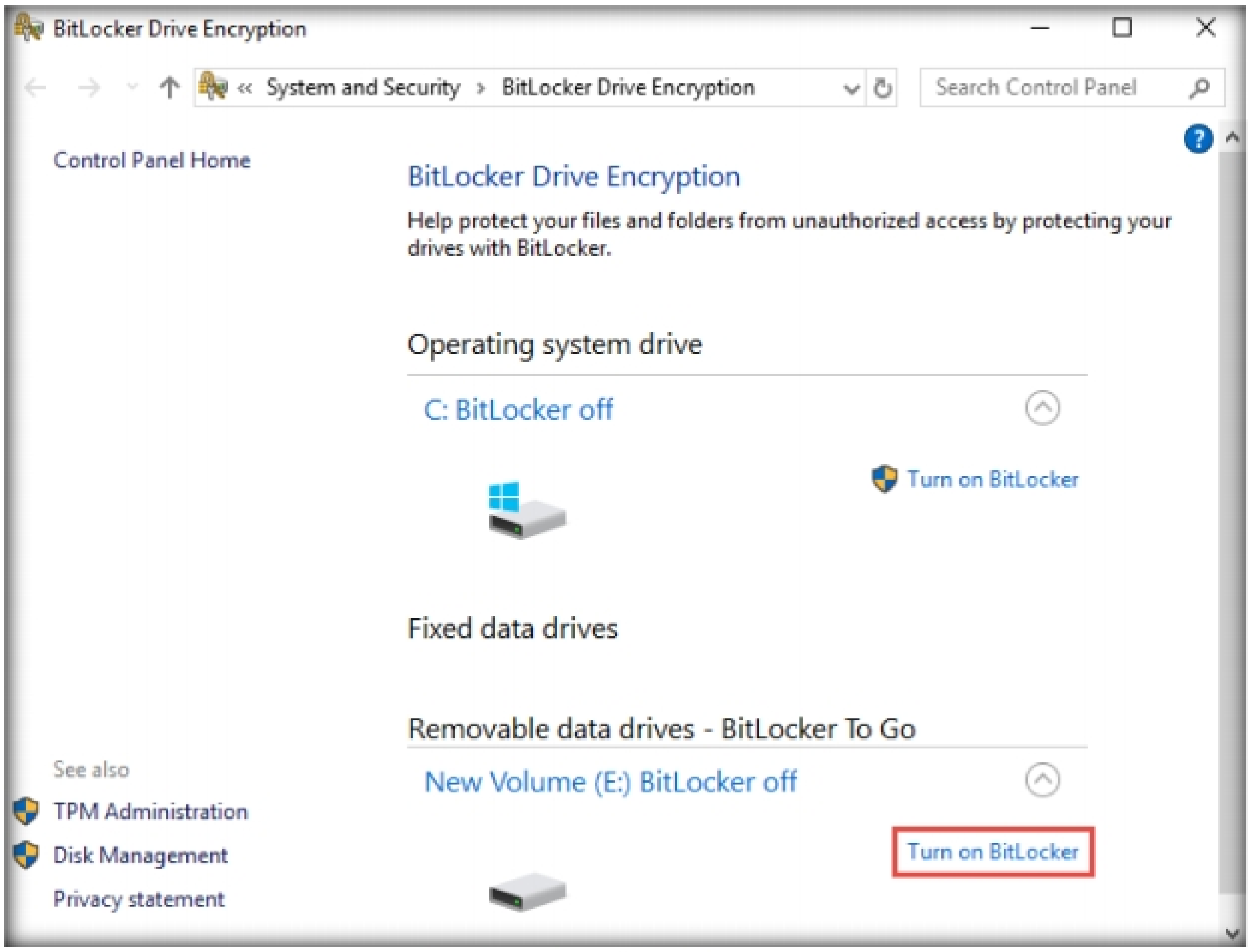
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Figure 4.2.2: BitLocker Drive Encryption

TASK 2.2

Encrypt the Drive

3. Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off**.

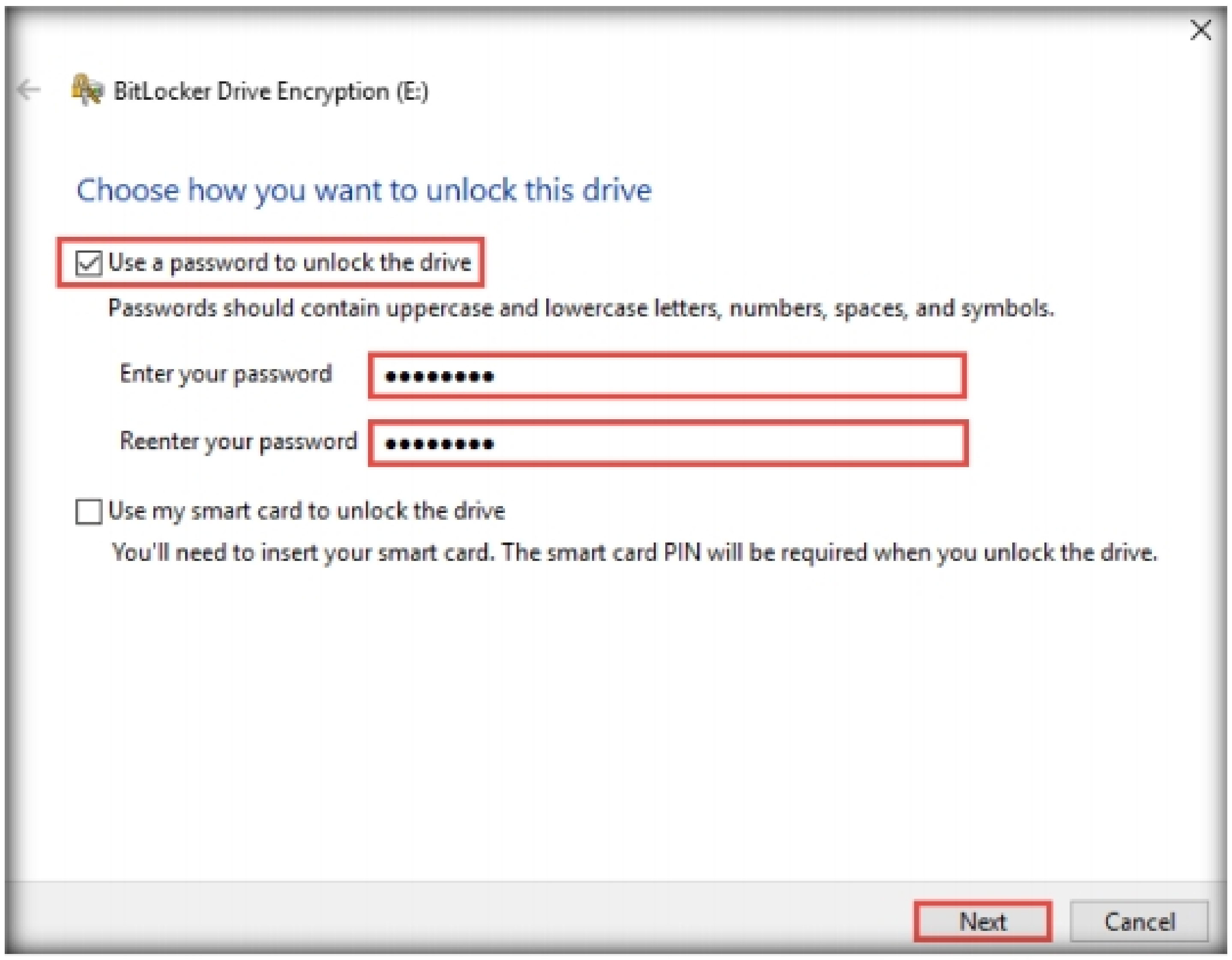

BitLocker Drive Encryption
« System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption
Operating system drive
C: BitLocker off
Turn on BitLocker
Fixed data drives
Removable data drives - BitLocker To Go
New Volume (E:) BitLocker off
Turn on BitLocker
See also
TPM Administration
Disk Management
Privacy statement

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Figure 4.2.3: Turn on BitLocker option

4. The **BitLocker Drive Encryption (E:)** wizard appears; check the **Use a password to unlock the drive** checkbox.

5. Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).



BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☑ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password: ••••••••

Reenter your password: ••••••••

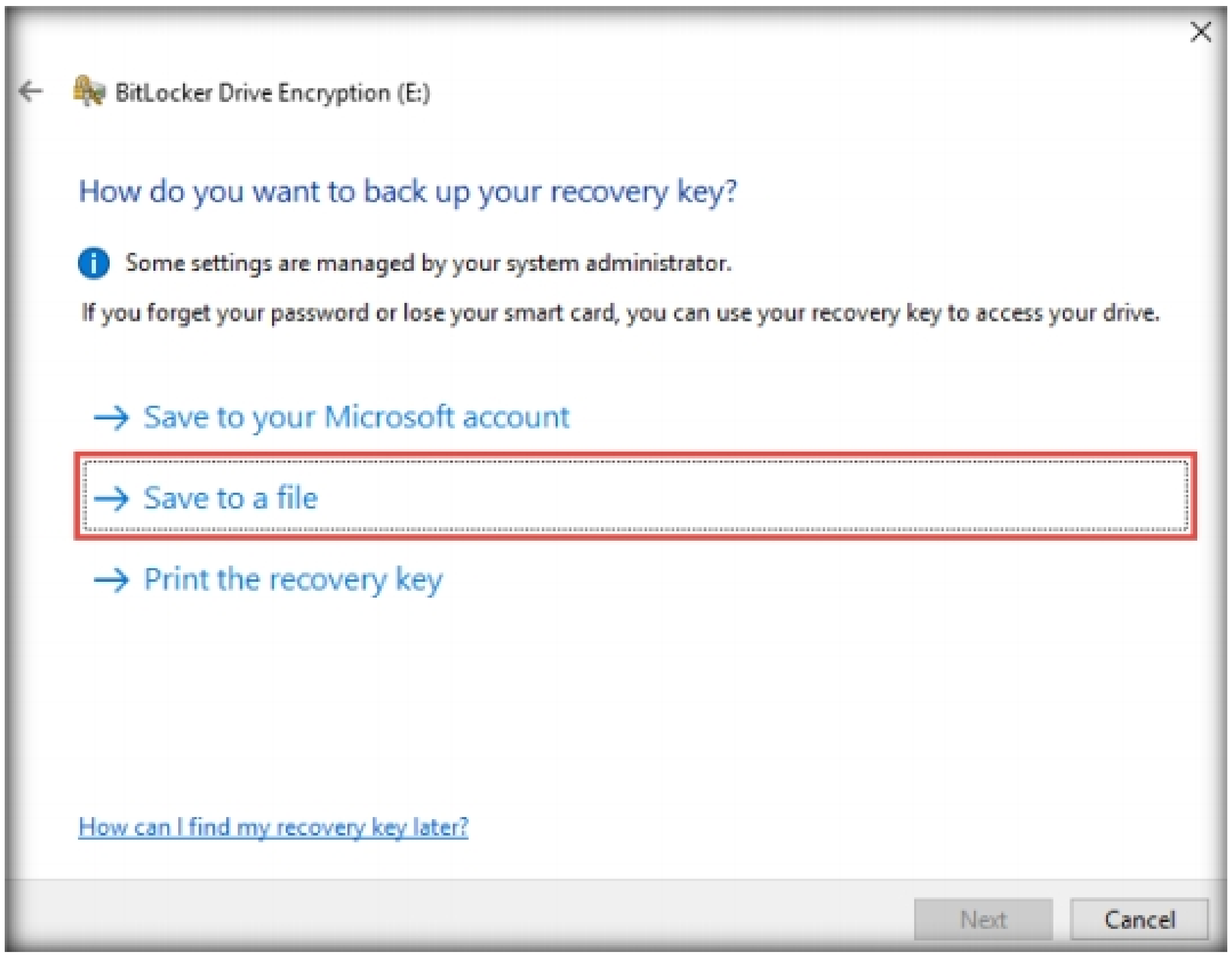
☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Next
Cancel

Figure 4.2.4: BitLocker Drive Encryption (E:) wizard

6. The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.



BitLocker Drive Encryption (E:)

How do you want to back up your recovery key?

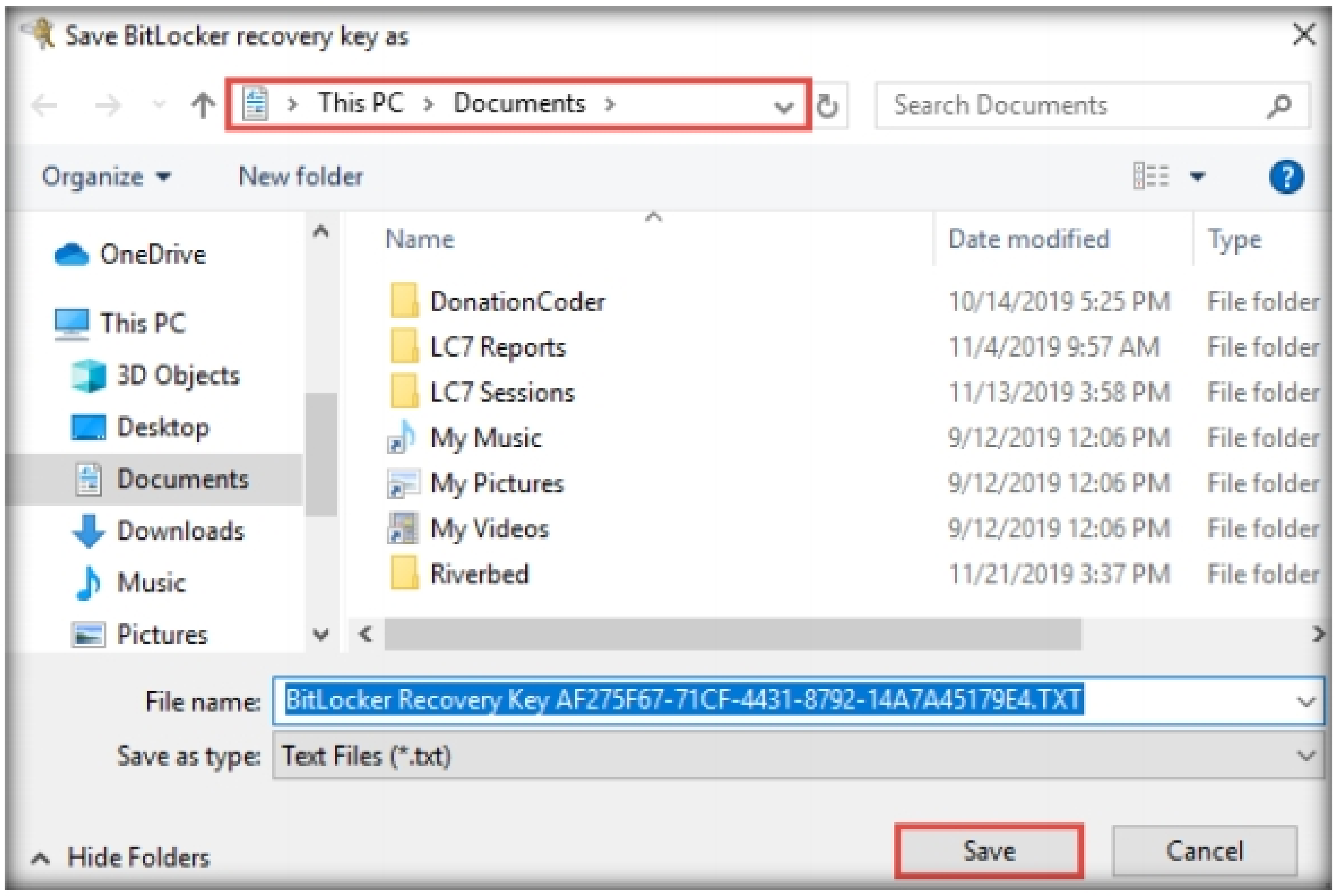
Some settings are managed by your system administrator.

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your Microsoft account
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

Figure 4.2.5: How do you want to back up your recovery key? step

7. The **Save BitLocker recovery key as** window appears; keep the save location set to default and click **Save**.


Save BitLocker recovery key as
This PC > Documents >
Search Documents
Organize
New folder
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Name
Date modified
Type
DonationCoder 10/14/2019 5:25 PM File folder
LC7 Reports 11/4/2019 9:57 AM File folder
LC7 Sessions 11/13/2019 3:58 PM File folder
My Music 9/12/2019 12:06 PM File folder
My Pictures 9/12/2019 12:06 PM File folder
My Videos 9/12/2019 12:06 PM File folder
Riverbed 11/21/2019 3:37 PM File folder
Hide Folders
Save
Cancel

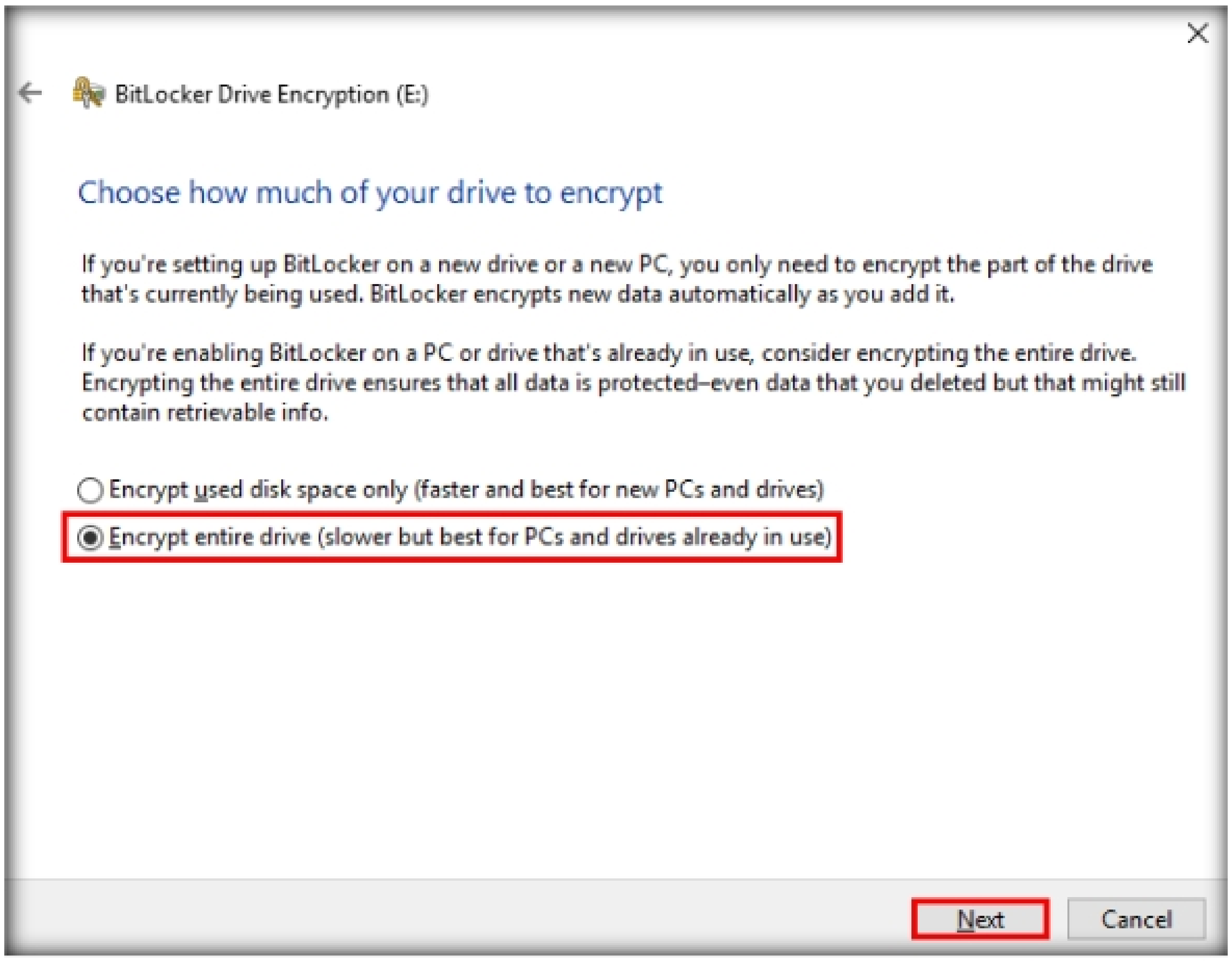
File name: BitLocker Recovery Key AF275F67-71CF-4431-8792-14A7A45179E4.TXT

Save as type: Text Files (*.txt)

Figure 4.2.6: How do you want to back up your recovery key? step

8. Click **Next** in the **How do you want to back up your recovery key?** step.

9. In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.


BitLocker Drive Encryption (E:)

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.

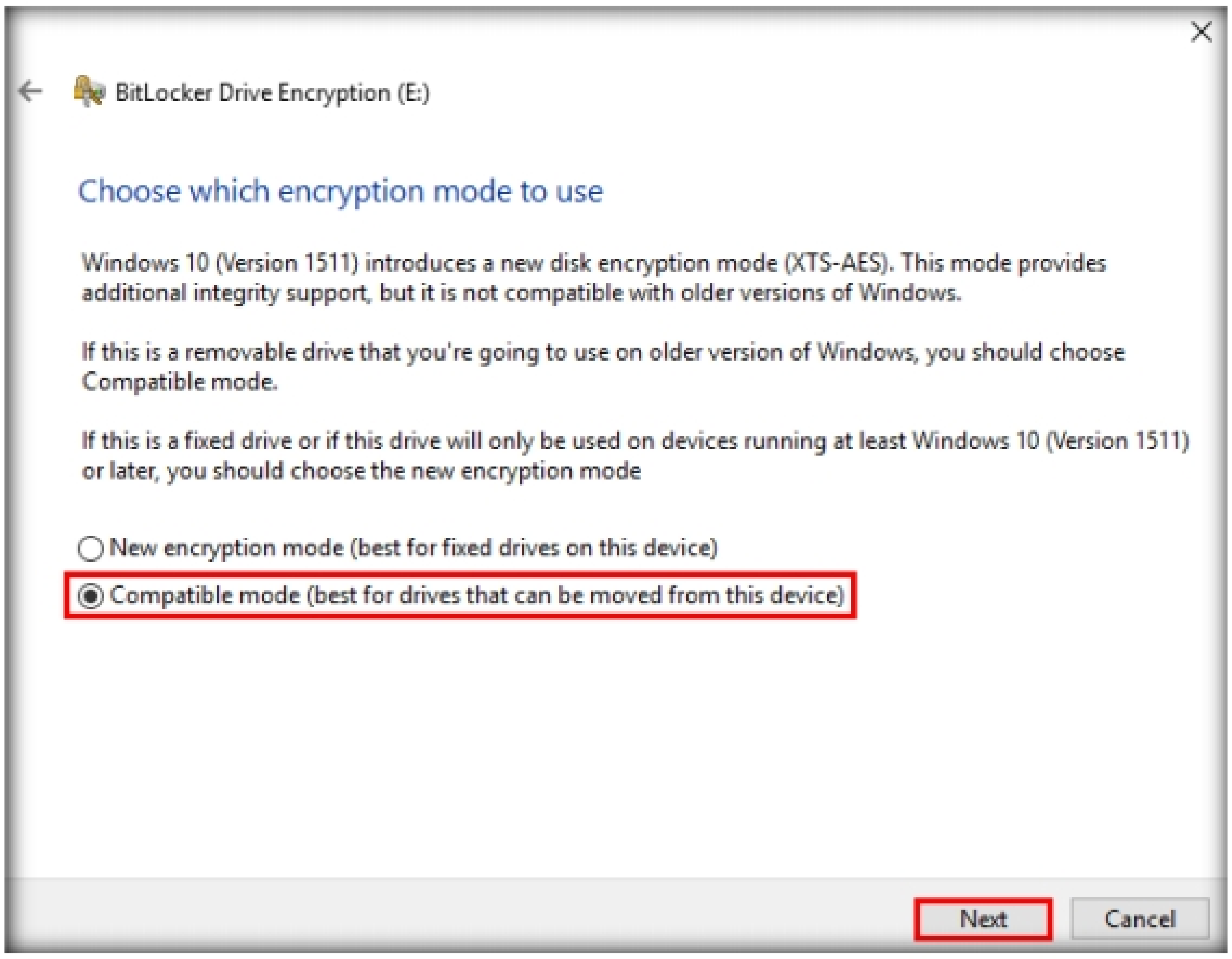
○ Encrypt used disk space only (faster and best for new PCs and drives)

● Encrypt entire drive (slower but best for PCs and drives already in use)

Next
Cancel

Figure 4.2.7: Choose how much of your drive to encrypt step

10. In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.



Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

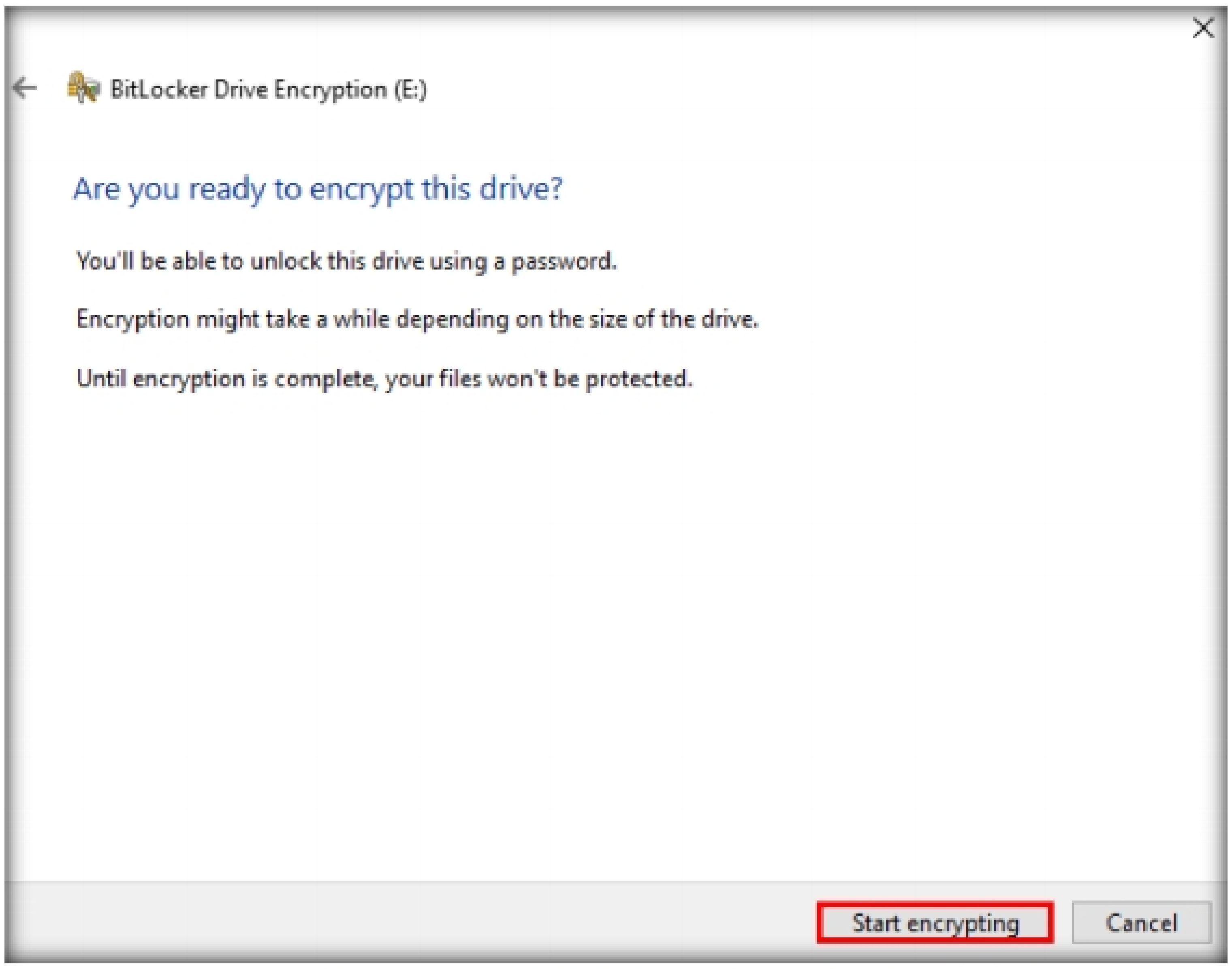
If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)
● Compatible mode (best for drives that can be moved from this device)

Figure 4.2.8: Choose which encryption mode to use step

11. In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.



Are you ready to encrypt this drive?

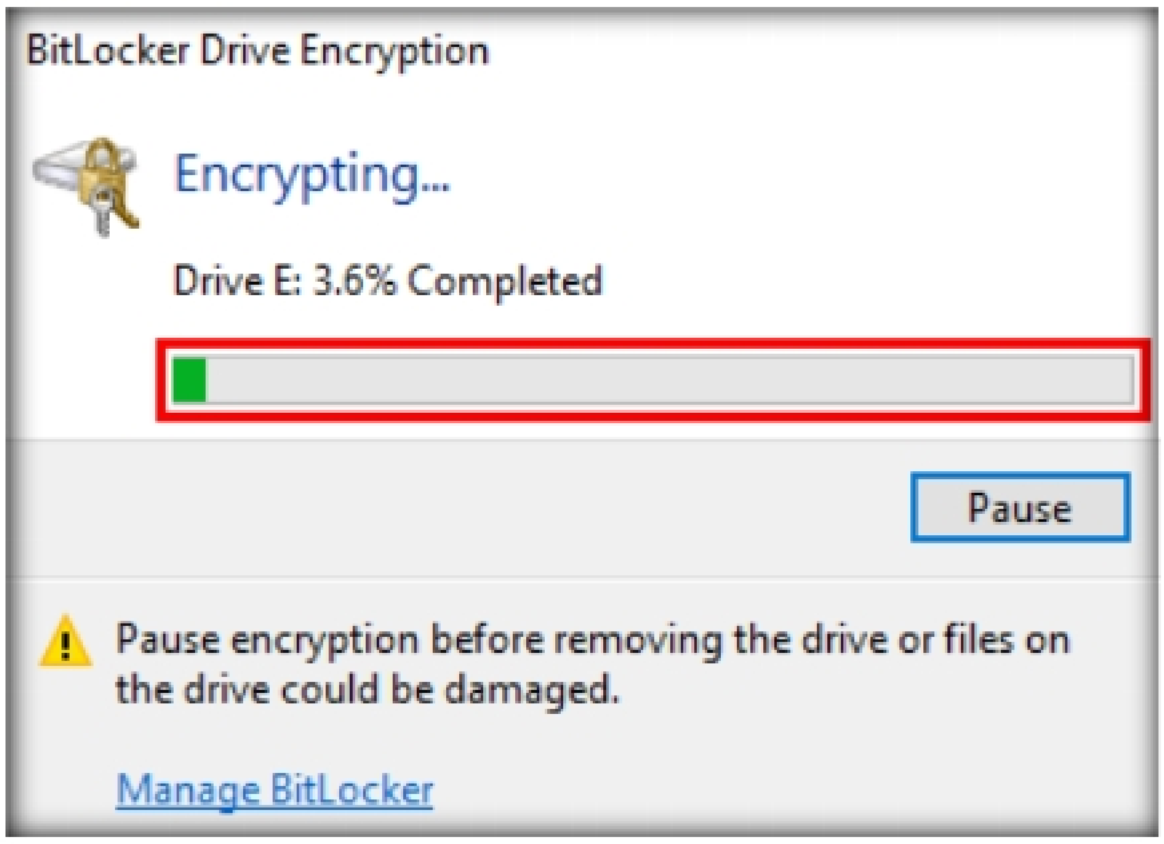
You'll be able to unlock this drive using a password.

Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.

Figure 4.2.9: Are you ready to encrypt this drive? steps

12. The **BitLocker Drive Encryption** pop-up appears, showing the **Encrypting...** status.



BitLocker Drive Encryption

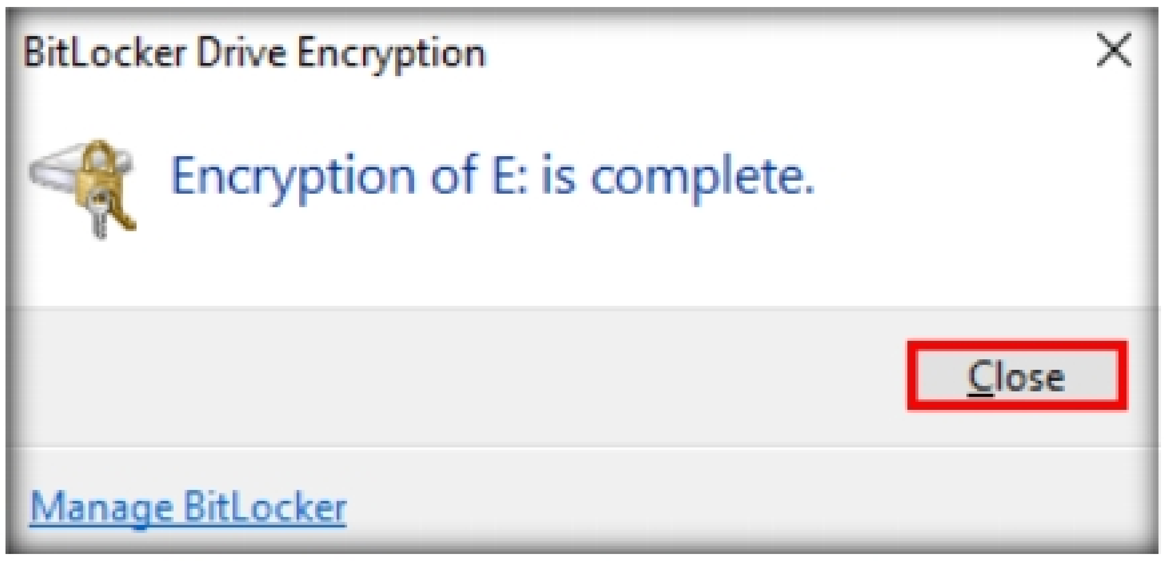
Encrypting...

Drive E: 3.6% Completed

Pause encryption before removing the drive or files on the drive could be damaged.

Figure 4.2.10: Encrypting pop-up

13. After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the virtual machine.



BitLocker Drive Encryption

Encryption of E: is complete.

Figure 4.2.11: Encryption of E: is complete notification

14. After the system reboots, log in with the credentials **Admin**/**Pa$$w0rd**.

TASK 2.3

Access the Encrypted Disk

15. Open **File Explorer** and click **This PC** from the left pane.

16. You can observe that **Local Disk (E:)** is now encrypted; double-click and the **BitLocker (E:)** security pop-up appears at the top-right corner of **Desktop**.

17. Type the password you provided in **Step#5** and click **Unlock**.

Note: Here, the password is **test@123**.

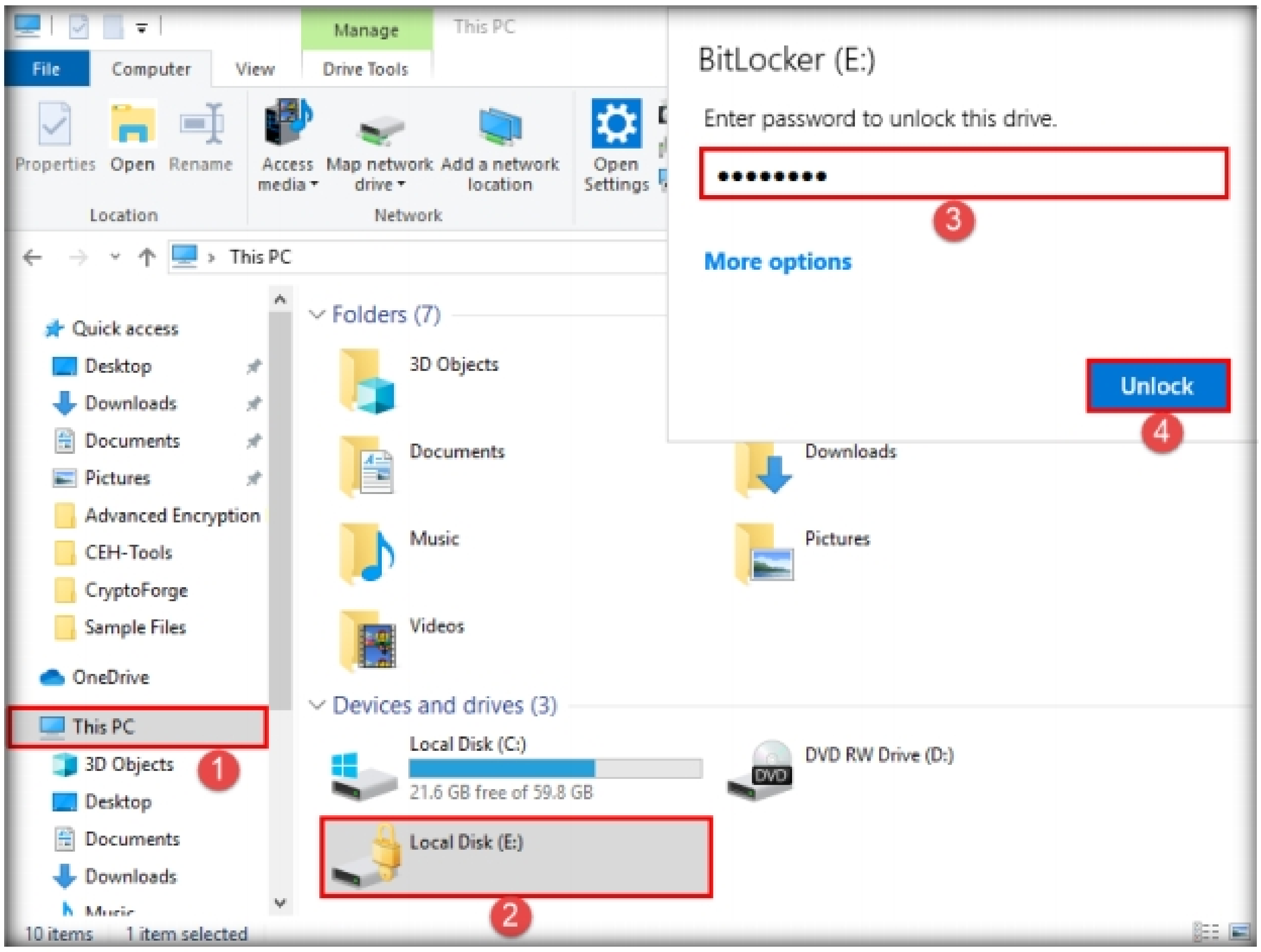

Manage
This PC
File
Computer
View
Drive Tools
Properties
Open
Rename
Access media
Map network drive
Add a network location
Open Settings
Location
Network
This PC
Quick access
Desktop
Downloads
Documents
Pictures
Advanced Encryption
CEH-Tools
CryptoForge
Sample Files
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Folders (7)
3D Objects
Documents
Downloads
Music
Pictures
Videos
Devices and drives (3)
Local Disk (C:)
21.6 GB free of 59.8 GB
DVD RW Drive (D:)
Local Disk (E:)
10 items
1 item selected
BitLocker (E:)
Enter password to unlock this drive.
••••••••
More options
Unlock
①
②
③
④

Figure 4.2.12: Accessing the encrypted disk

18. The **New Volume (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

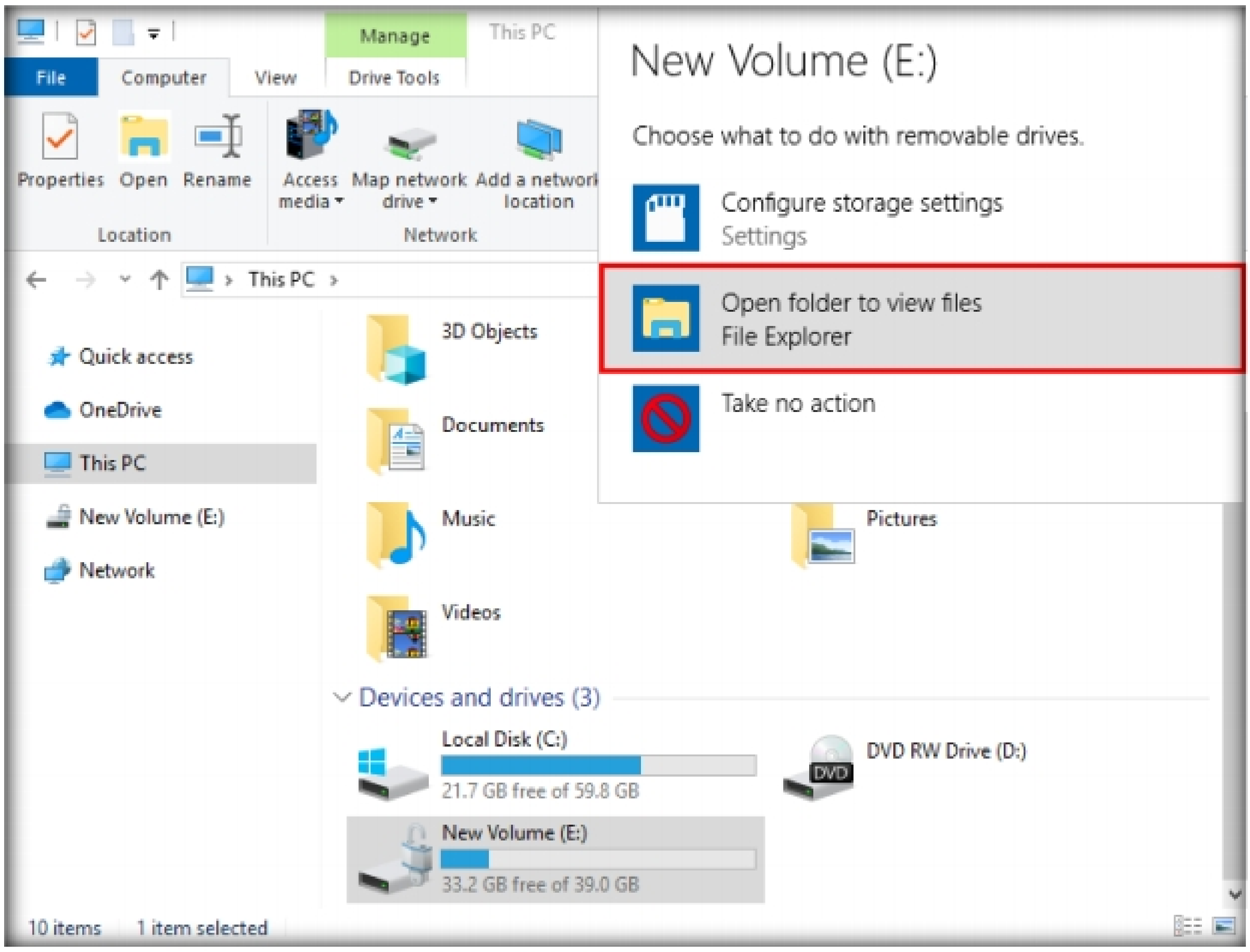
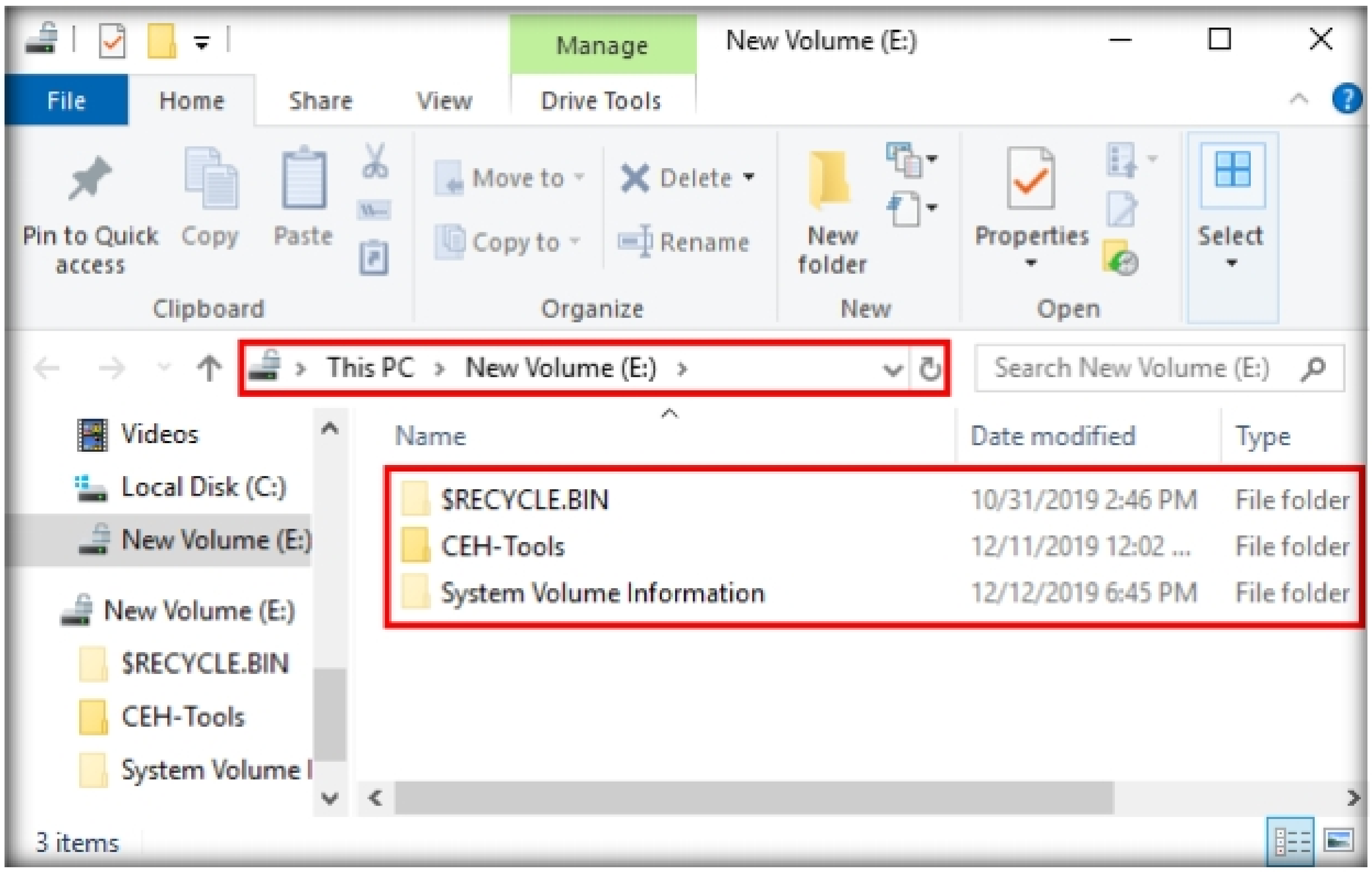

Manage
This PC
File
Computer
View
Drive Tools
Properties
Open
Rename
Access media
Map network drive
Add a network location
Location
Network
This PC
Quick access
OneDrive
This PC
New Volume (E:)
Network
3D Objects
Documents
Music
Pictures
Videos
Devices and drives (3)
Local Disk (C:)
21.7 GB free of 59.8 GB
DVD RW Drive (D:)
New Volume (E:)
33.2 GB free of 39.0 GB
10 items
1 item selected
New Volume (E:)
Choose what to do with removable drives.
Configure storage settings
Settings
Open folder to view files
File Explorer
Take no action

Figure 4.2.13: New Volume (E:) pop-up

19. The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

Note: The disk will remain unlocked until the next time you restart the system.


Manage
New Volume (E:)
File
Home
Share
View
Drive Tools
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select
Clipboard
Organize
New
Open
This PC > New Volume (E:) >
Search New Volume (E:)
Videos
Local Disk (C:)
New Volume (E:)
New Volume (E:)
$RECYCLE.BIN
CEH-Tools
System Volume I
3 items

Name	Date modified	Type
$RECYCLE.BIN	10/31/2019 2:46 PM	File folder
CEH-Tools	12/11/2019 12:02 ...	File folder
System Volume Information	12/12/2019 6:45 PM	File folder

Figure 4.2.14: New Volume (E:) disk content

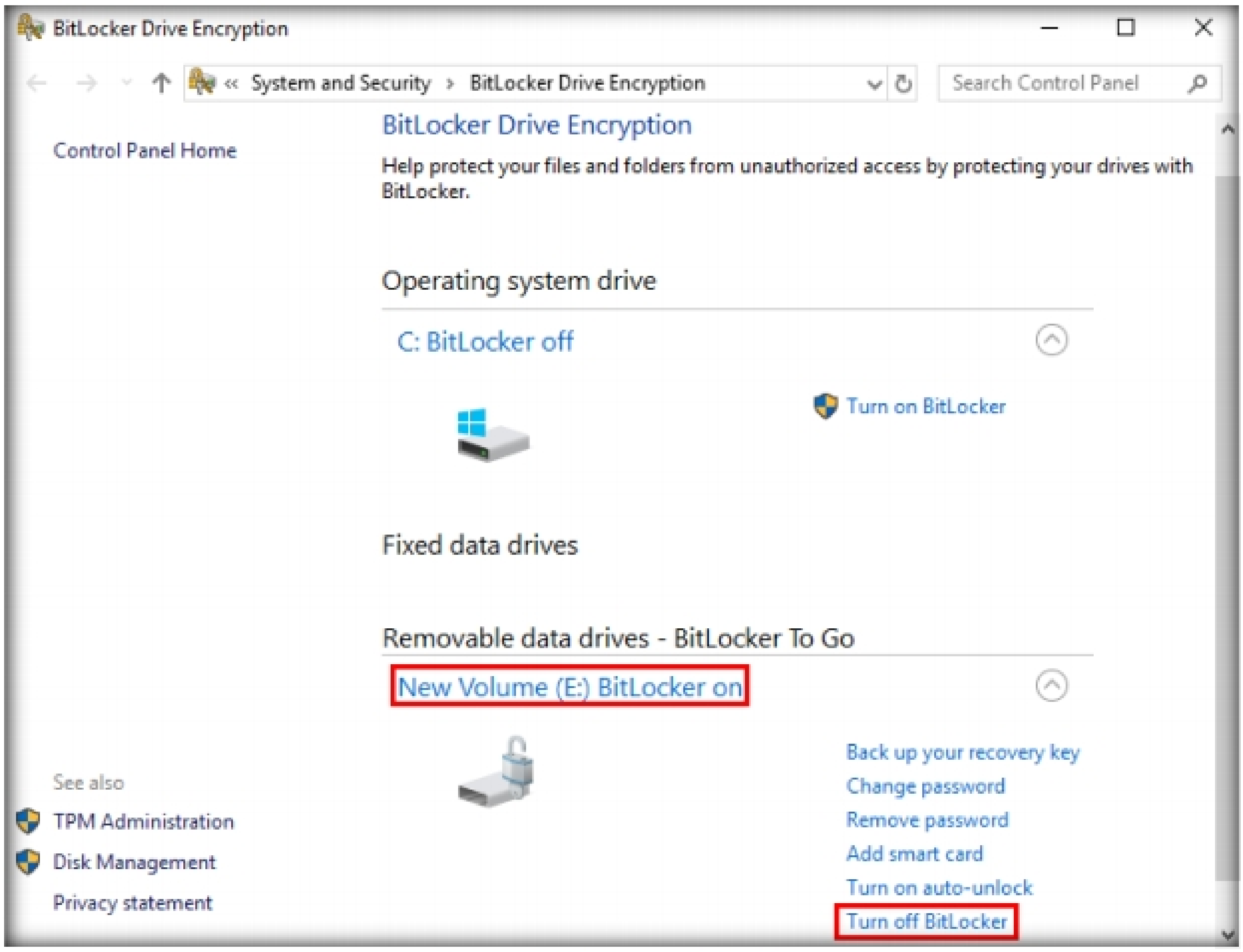
20. This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.

21. Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.

TASK 2.4

Turn off BitLocker

22. To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker**.



BitLocker Drive Encryption

System and Security > BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

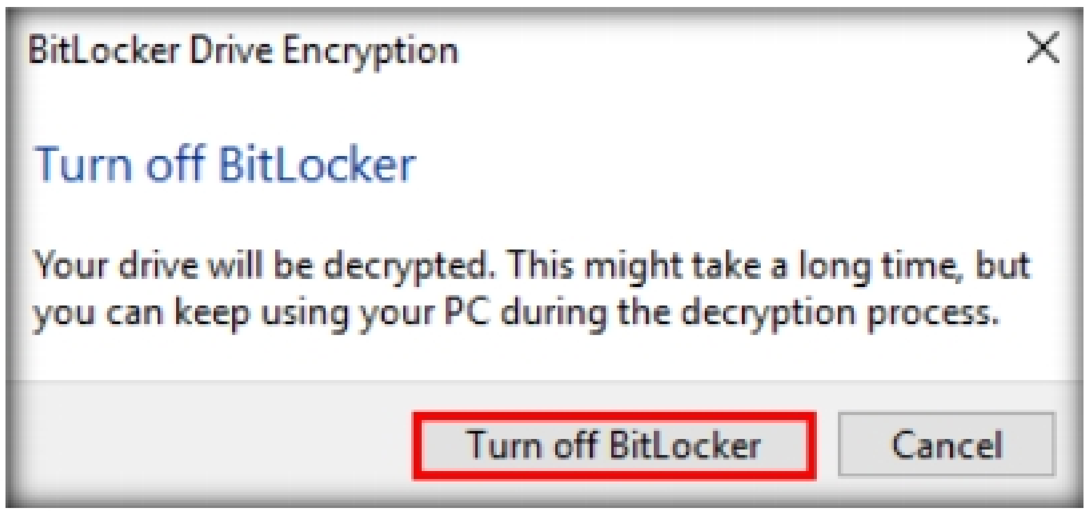
New Volume (E:) BitLocker on

Back up your recovery key
Change password
Remove password
Add smart card
Turn on auto-unlock
Turn off BitLocker

See also
TPM Administration
Disk Management
Privacy statement

Figure 4.2.15: Turn off BitLocker

23. The **BitLocker Drive Encryption** pop-up appears; click **Turn off BitLocker**.



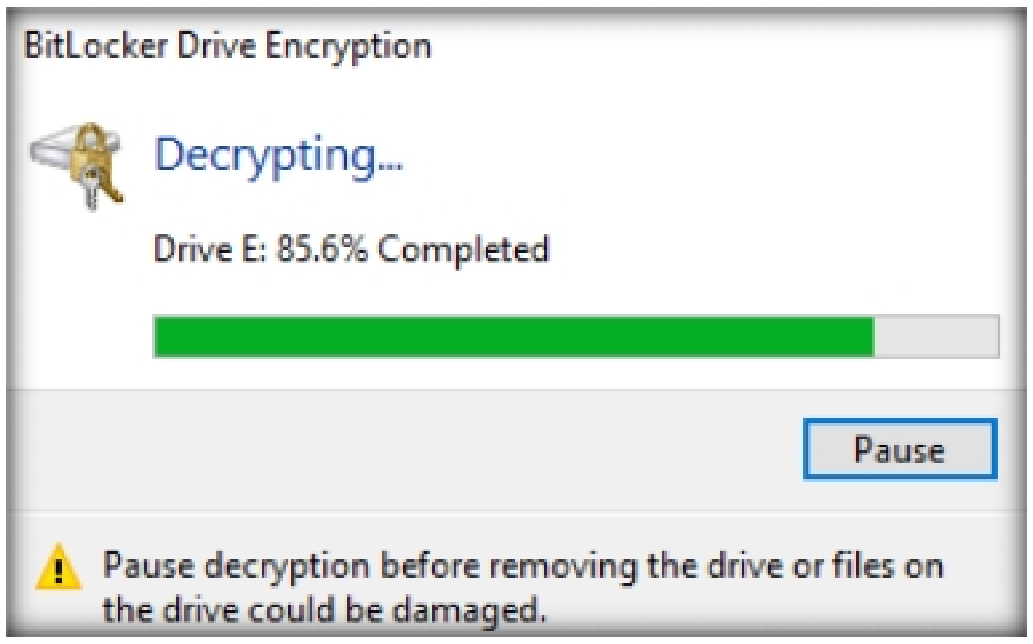
BitLocker Drive Encryption

Turn off BitLocker

Your drive will be decrypted. This might take a long time, but you can keep using your PC during the decryption process.

Figure 4.2.16: BitLocker Drive Encryption pop-up

24. **BitLocker** initiates the decryption process. Wait for it to complete.



BitLocker Drive Encryption

Decrypting...

Drive E: 85.6% Completed

Pause decryption before removing the drive or files on the drive could be damaged.

Figure 4.2.17: BitLocker Decrypting drive

25. After the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.

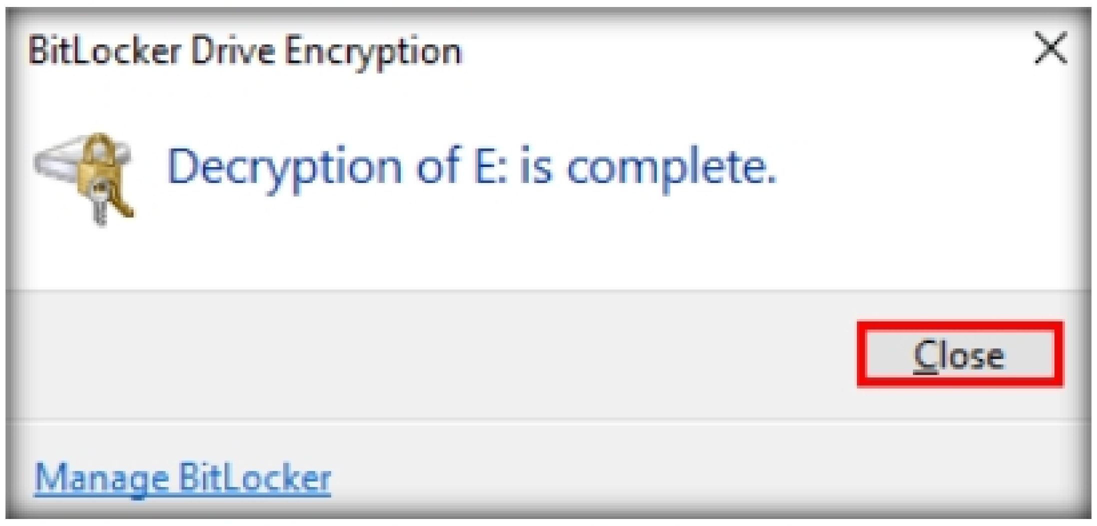

BitLocker Drive Encryption
Decryption of E: is complete.
Close
Manage BitLocker

Figure 4.2.18: Decryption of E: is complete pop-up

26. The **New Volume (E:)** decrypts successfully.

27. Close all open windows and document all the acquired information.

TASK 3

Perform Disk Encryption using Rohos Disk Encryption

Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

TASK 3.1

Install and Launch Rohos Disk Encryption

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

2. The **Select Setup Language** dialog box appears; click **OK**.

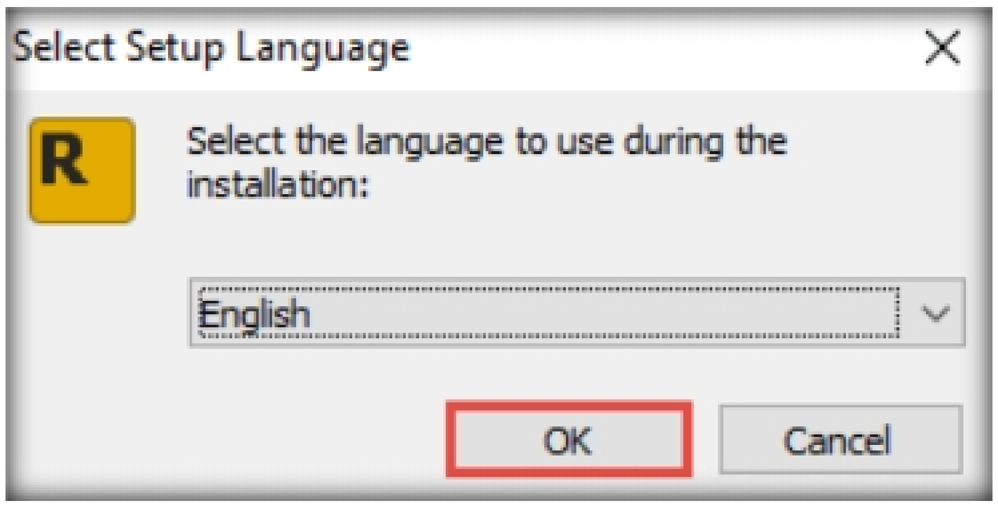
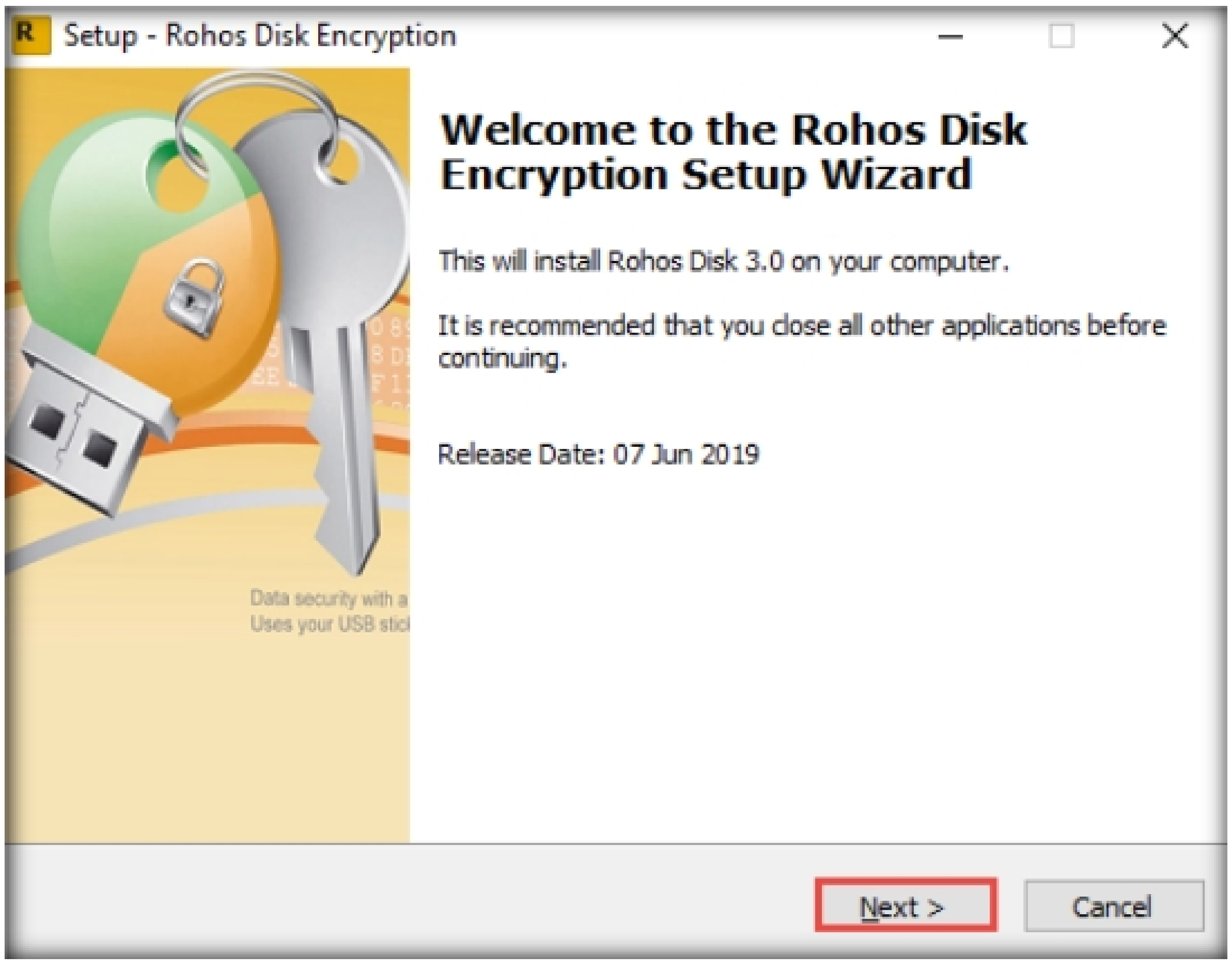

Select Setup Language
Select the language to use during the installation:
English
OK
Cancel

Figure 4.3.1: Select the Language

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

3. The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.



Setup - Rohos Disk Encryption

Welcome to the Rohos Disk Encryption Setup Wizard

This will install Rohos Disk 3.0 on your computer.

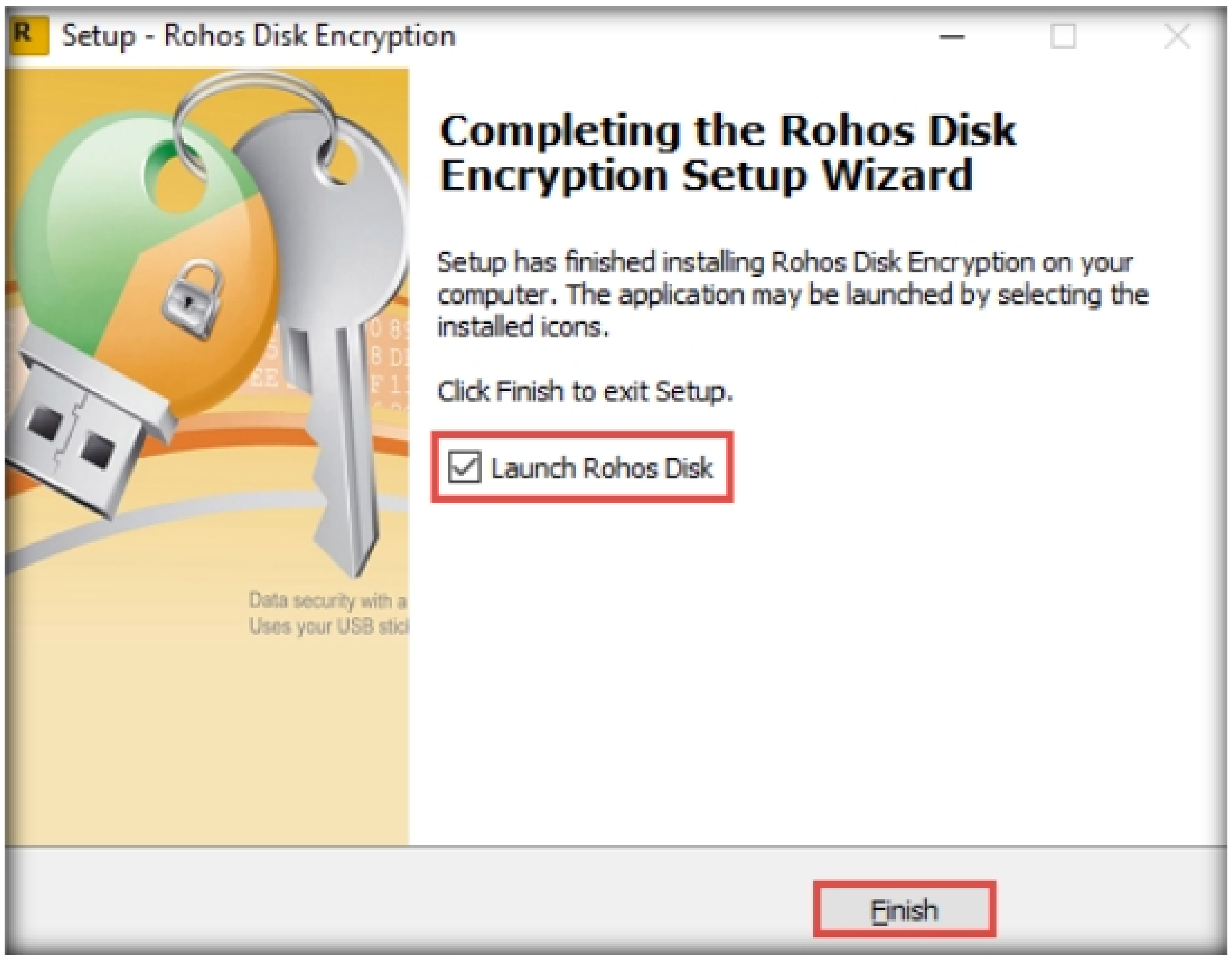
It is recommended that you close all other applications before continuing.

Release Date: 07 Jun 2019

Figure 4.3.2: Rohos setup wizard

4. Follow the steps and install the application using all default settings.

5. After the completion of the installation, **Completing the Rohos Disk Encryption Setup Wizard** appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.



Setup - Rohos Disk Encryption

Completing the Rohos Disk Encryption Setup Wizard

Setup has finished installing Rohos Disk Encryption on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch Rohos Disk

Figure 4.3.3: License agreement window

TASK 3.2

Create an Encrypted Disk for Local Machine

6. The **Rohos Disk Encryption** main window appears; click **Create new disk...**

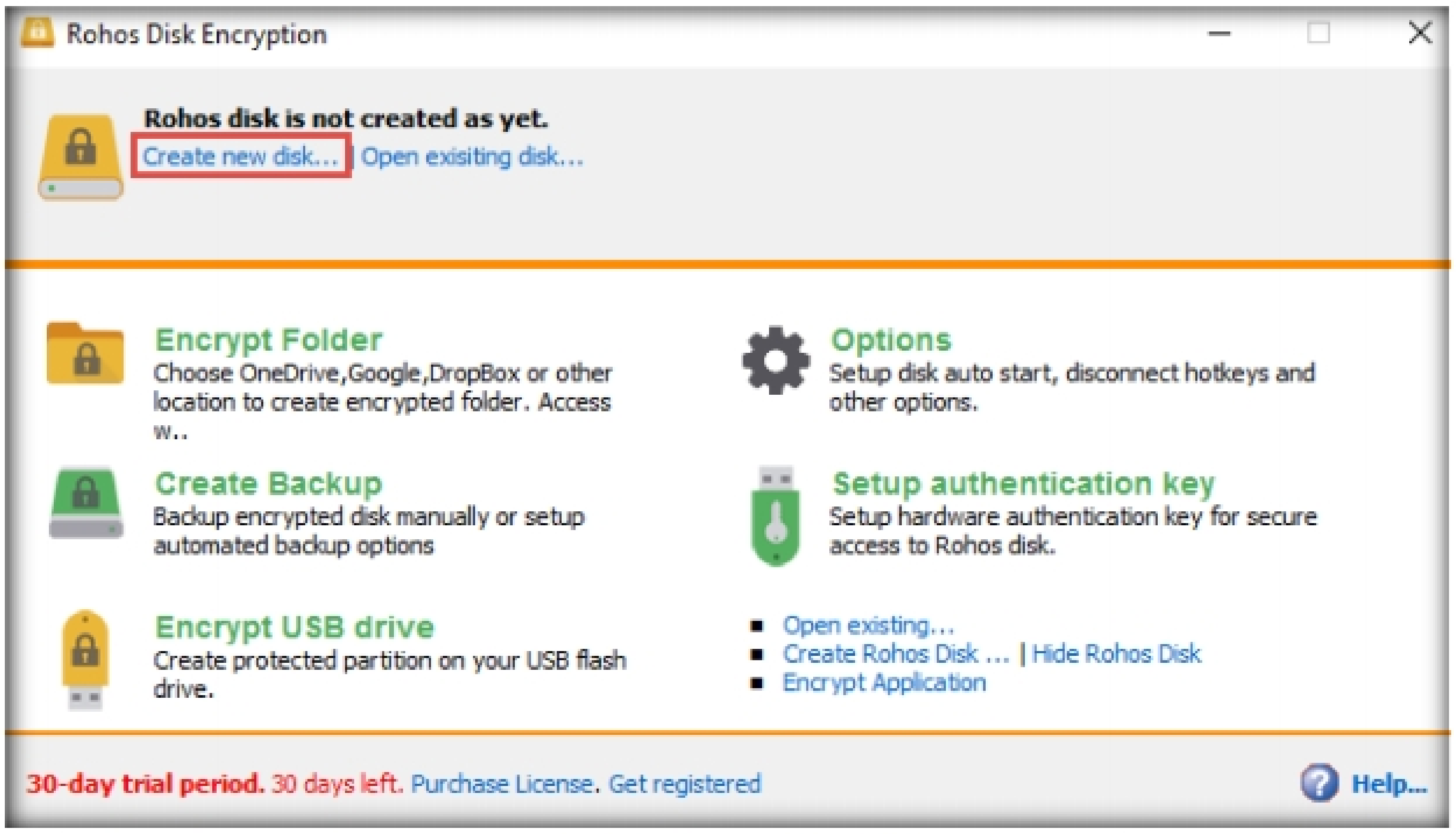
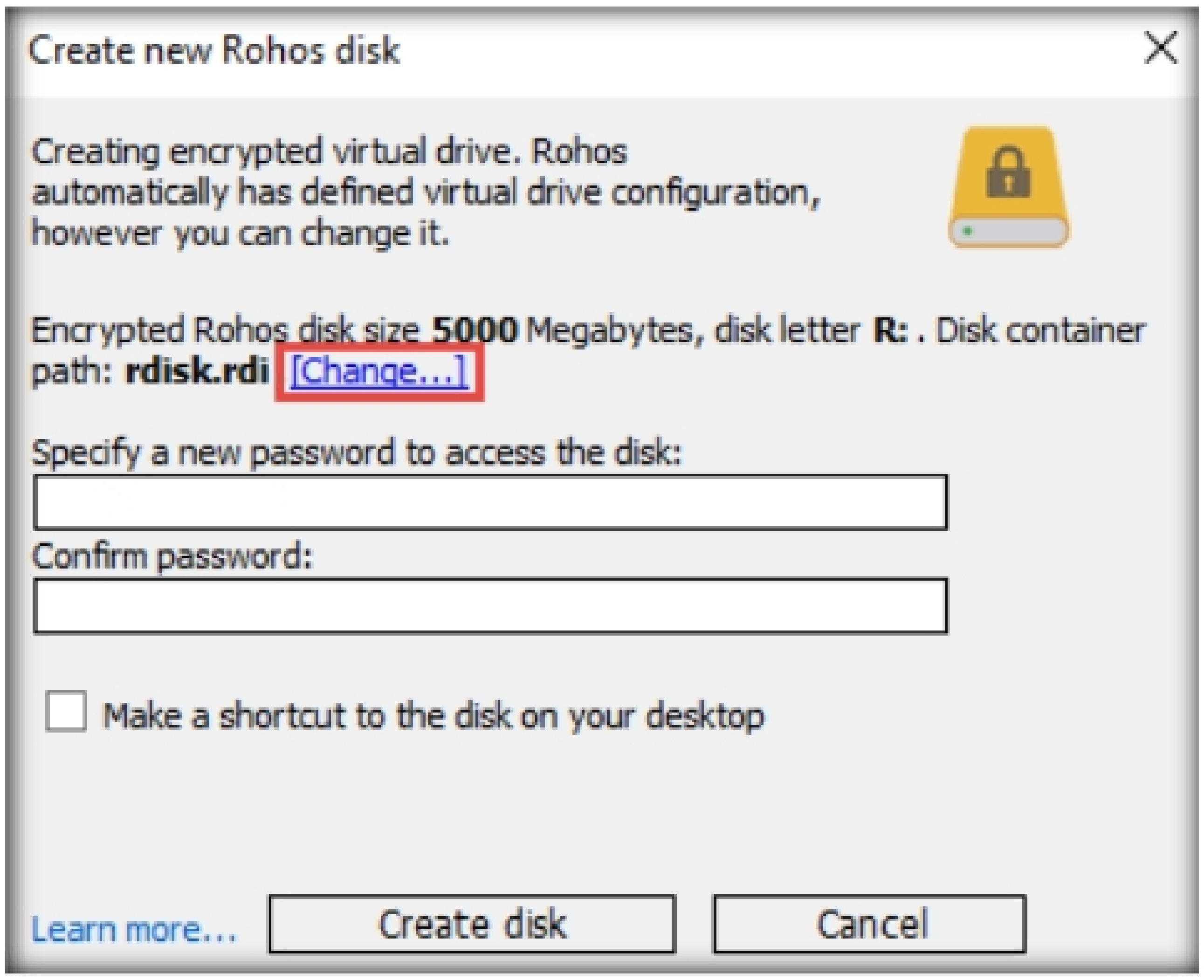

Rohos Disk Encryption
Rohos disk is not created as yet.
Create new disk...
Open exisiting disk...
Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..
Options
Setup disk auto start, disconnect hotkeys and other options.
Create Backup
Backup encrypted disk manually or setup automated backup options
Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.
Encrypt USB drive
Create protected partition on your USB flash drive.
Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application
30-day trial period. 30 days left. Purchase License. Get registered
Help...

Figure 4.3.4: Create new disk

7. The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.


Create new Rohos disk

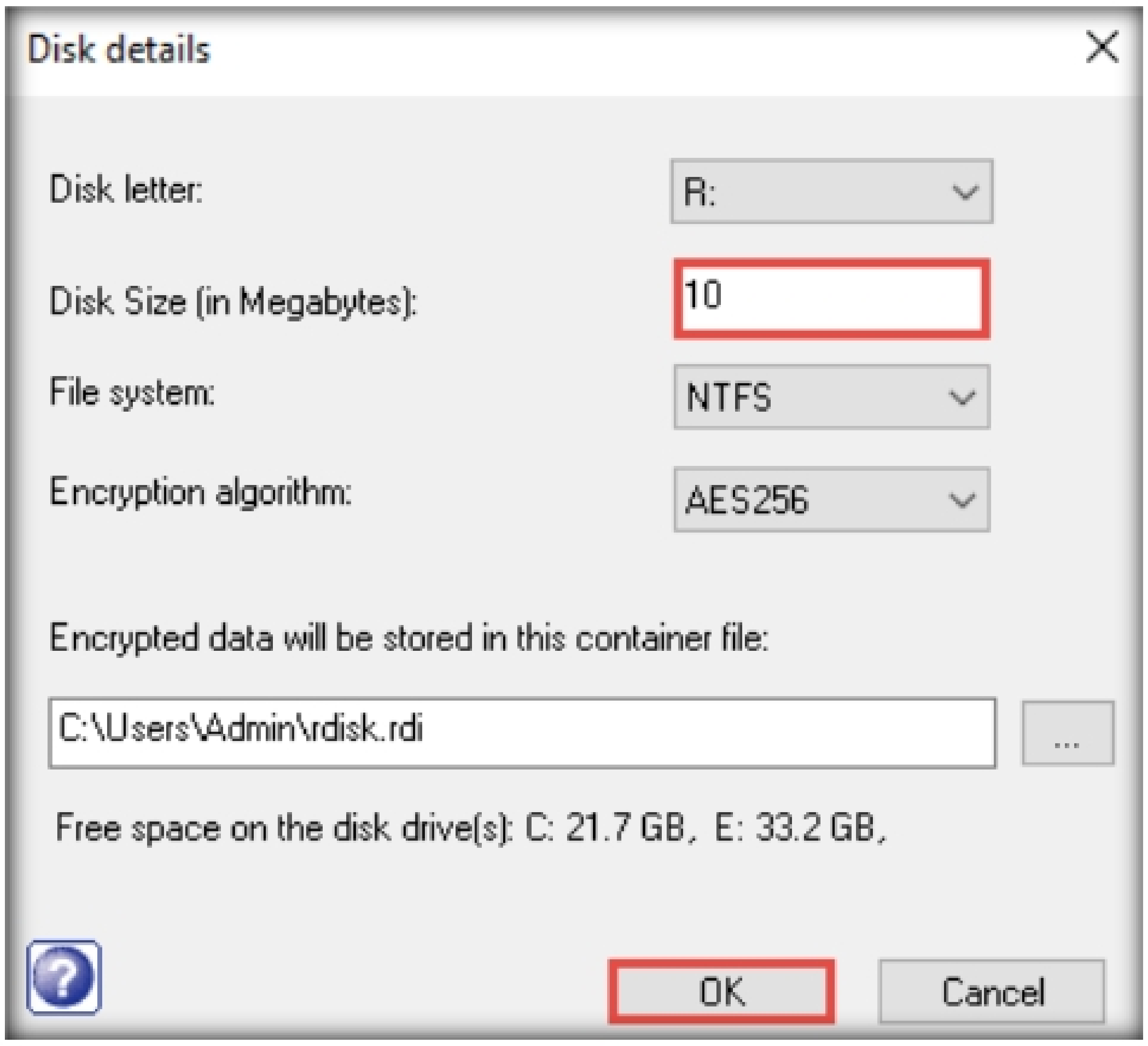
Creating encrypted virtual drive. Rohos automatically has defined virtual drive configuration, however you can change it.

Encrypted Rohos disk size **5000** Megabytes, disk letter **R:** . Disk container path: **rdisk.rdi** [Change...]

Specify a new password to access the disk:
Confirm password:
☐ Make a shortcut to the disk on your desktop
Learn more...
Create disk
Cancel

Figure 4.3.5: Create new Rohos disk window

8. The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.



Disk details

Disk letter: R:

Disk Size (in Megabytes): 10

File system: NTFS

Encryption algorithm: AES256

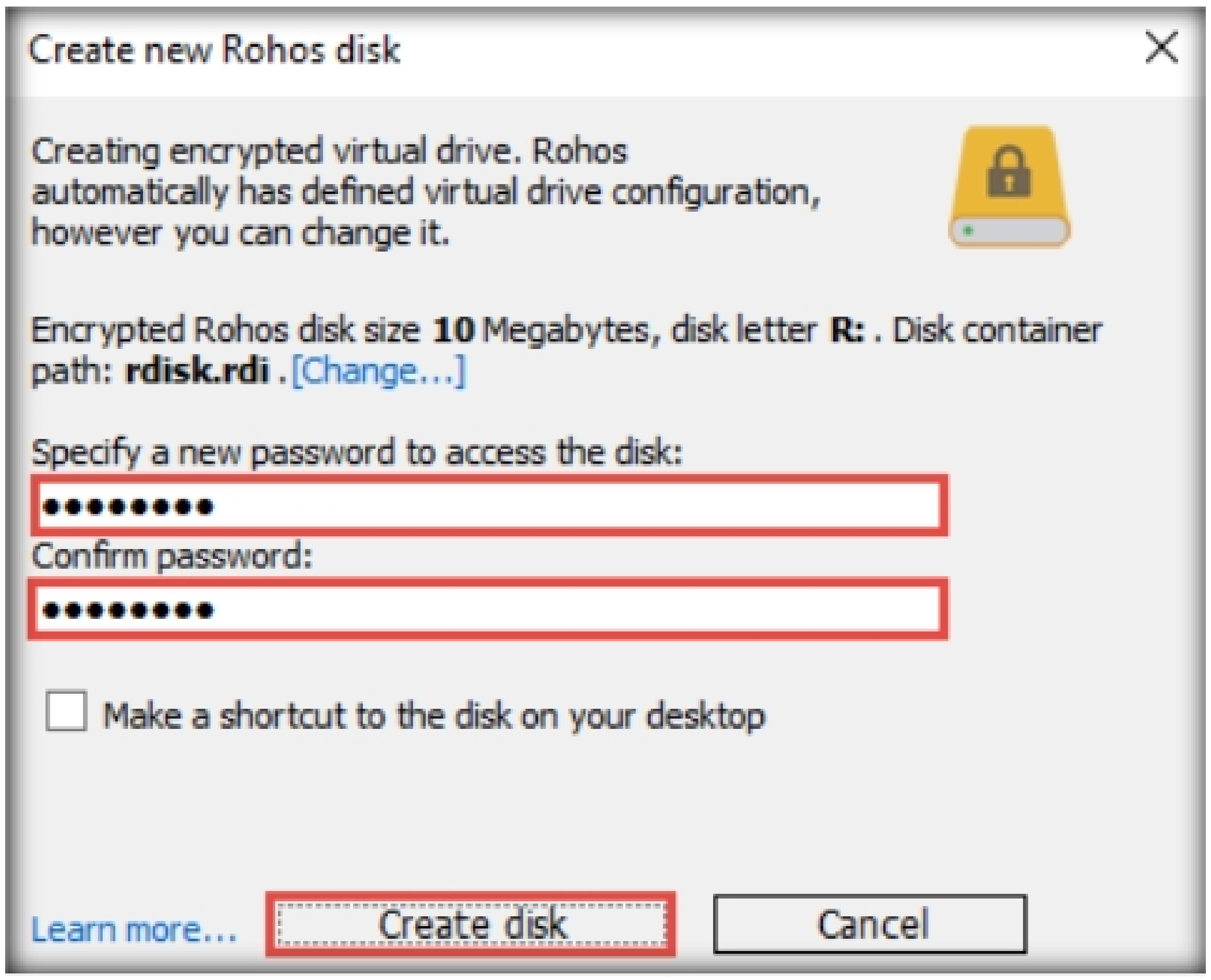
Encrypted data will be stored in this container file:

C:\Users\Admin\rdisk.rdi

Free space on the disk drive(s): C: 21.7 GB, E: 33.2 GB,

Figure 4.3.6: Disk details window

9. Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).



Create new Rohos disk

Creating encrypted virtual drive. Rohos automatically has defined virtual drive configuration, however you can change it.

Encrypted Rohos disk size **10** Megabytes, disk letter **R:** . Disk container path: **rdisk.rdi** . [Change...]

Specify a new password to access the disk: ••••••••

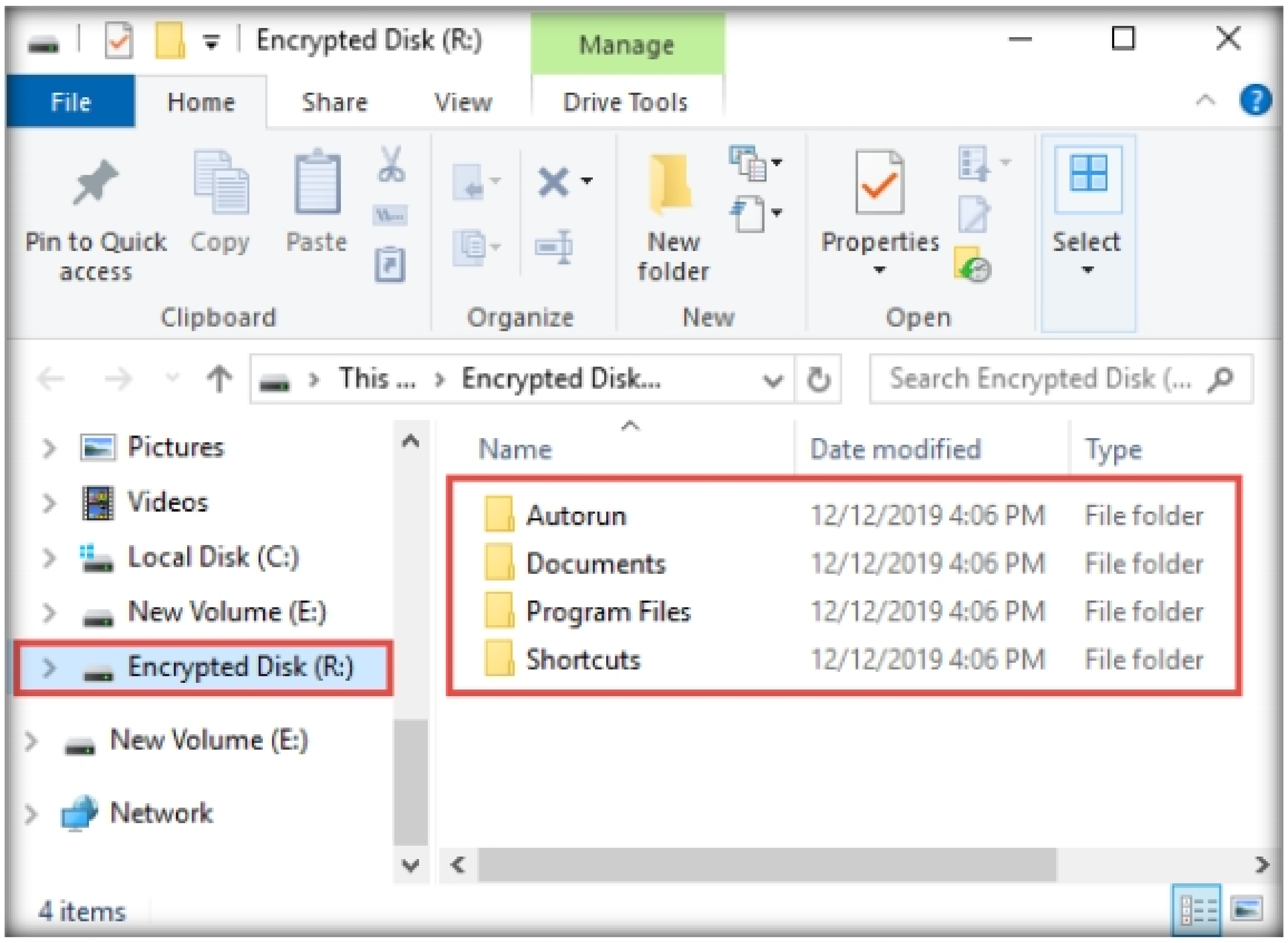
Confirm password: ••••••••

☐ Make a shortcut to the disk on your desktop

Figure 4.3.7: Specify password

10. Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.

11. On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.

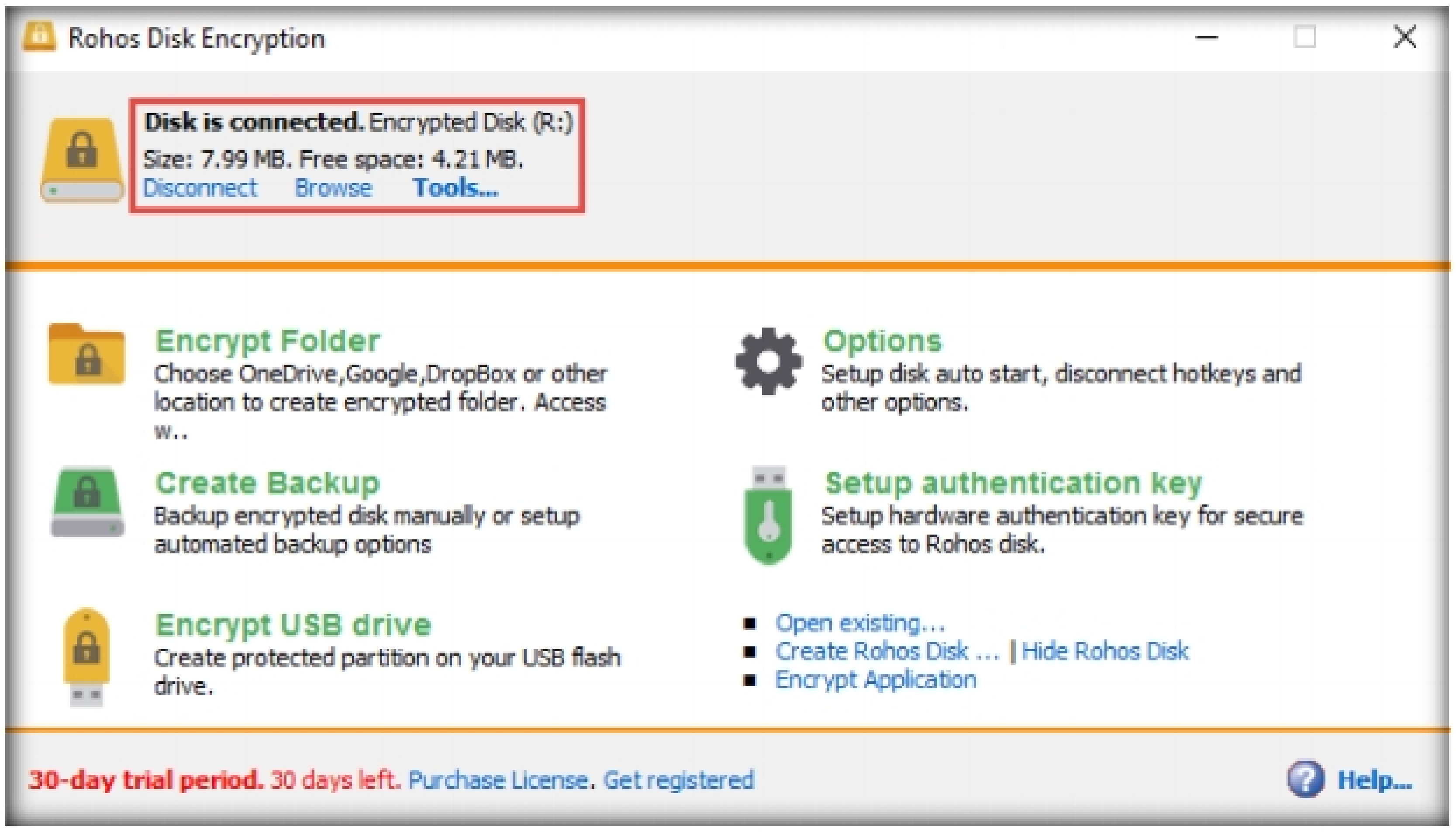

Encrypted Disk (R:)
Manage
File
Home
Share
View
Drive Tools
Pin to Quick access
Copy
Paste
Clipboard
Organize
New folder
New
Properties
Open
Select
This ... › Encrypted Disk...
Search Encrypted Disk (...
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Encrypted Disk (R:)
New Volume (E:)
Network
4 items

Name	Date modified	Type
Autorun	12/12/2019 4:06 PM	File folder
Documents	12/12/2019 4:06 PM	File folder
Program Files	12/12/2019 4:06 PM	File folder
Shortcuts	12/12/2019 4:06 PM	File folder

Figure 4.3.8: Encrypted disk successfully created

12. The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

Note: This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.


Rohos Disk Encryption
Disconnect
Browse
Tools...
Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application
Help...

Disk is connected. Encrypted Disk (R:)
Size: 7.99 MB. Free space: 4.21 MB.

Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Options
Setup disk auto start, disconnect hotkeys and other options.

Create Backup
Backup encrypted disk manually or setup automated backup options

Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.

Encrypt USB drive
Create protected partition on your USB flash drive.

30-day trial period. 30 days left. Purchase License. Get registered

Figure 4.3.9: Disk is connected notification

13. If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).

TASK 3.3

Create a File and Save it in Encrypted Disk

14. Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.

15. Click **File** in the menu bar and click **Save**.

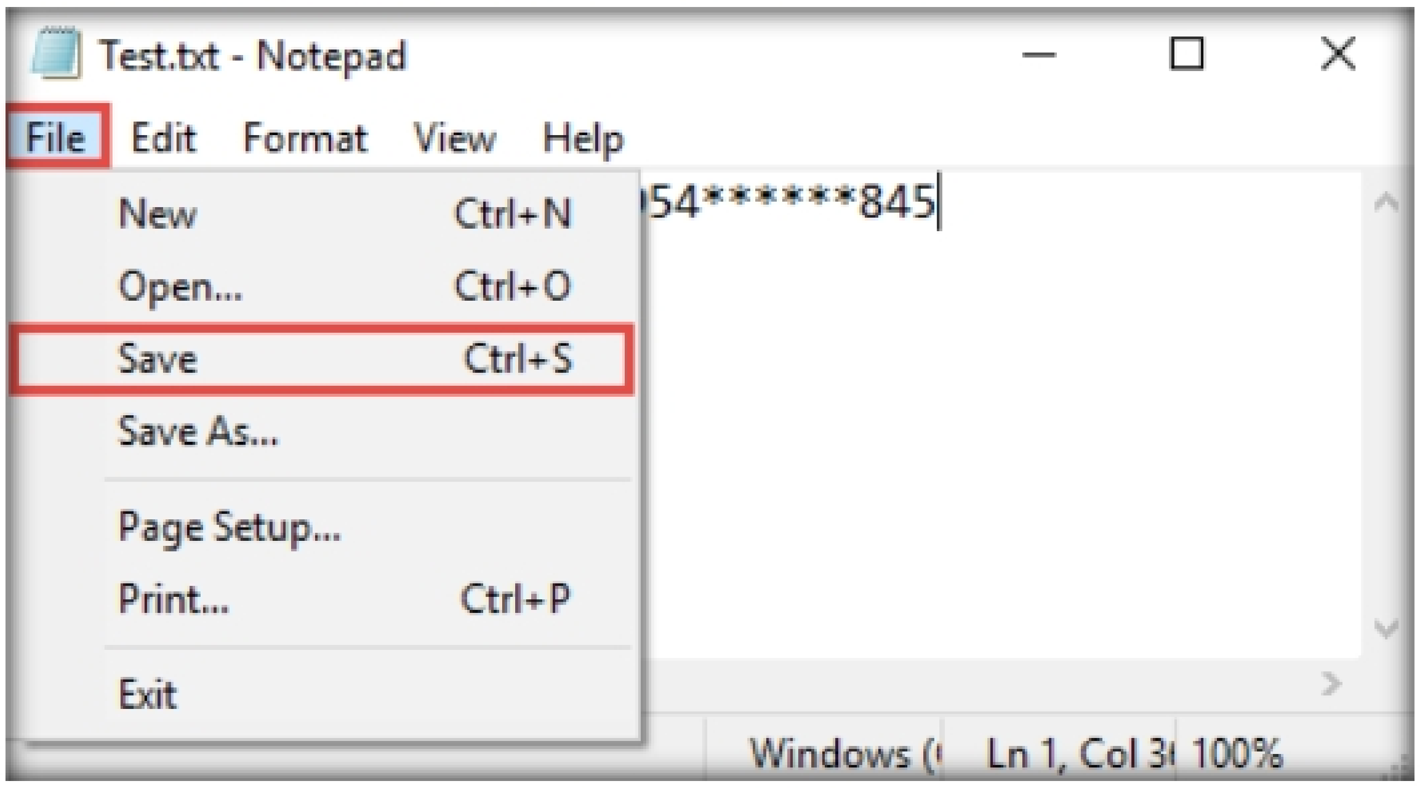
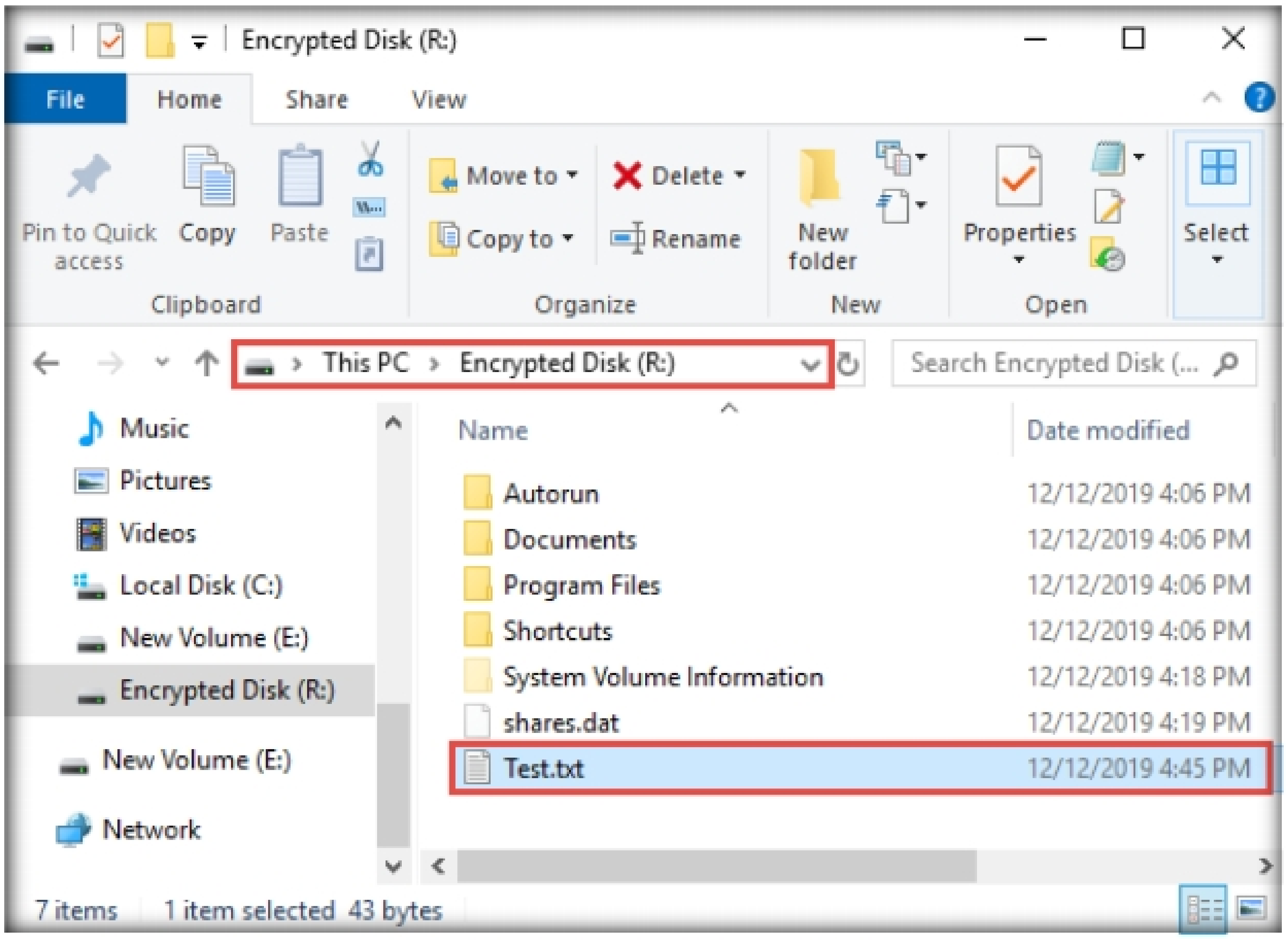

Test.txt - Notepad
File
Edit
Format
View
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
54******845
Windows (
Ln 1, Col 3
100%

Figure 4.3.10: Text file

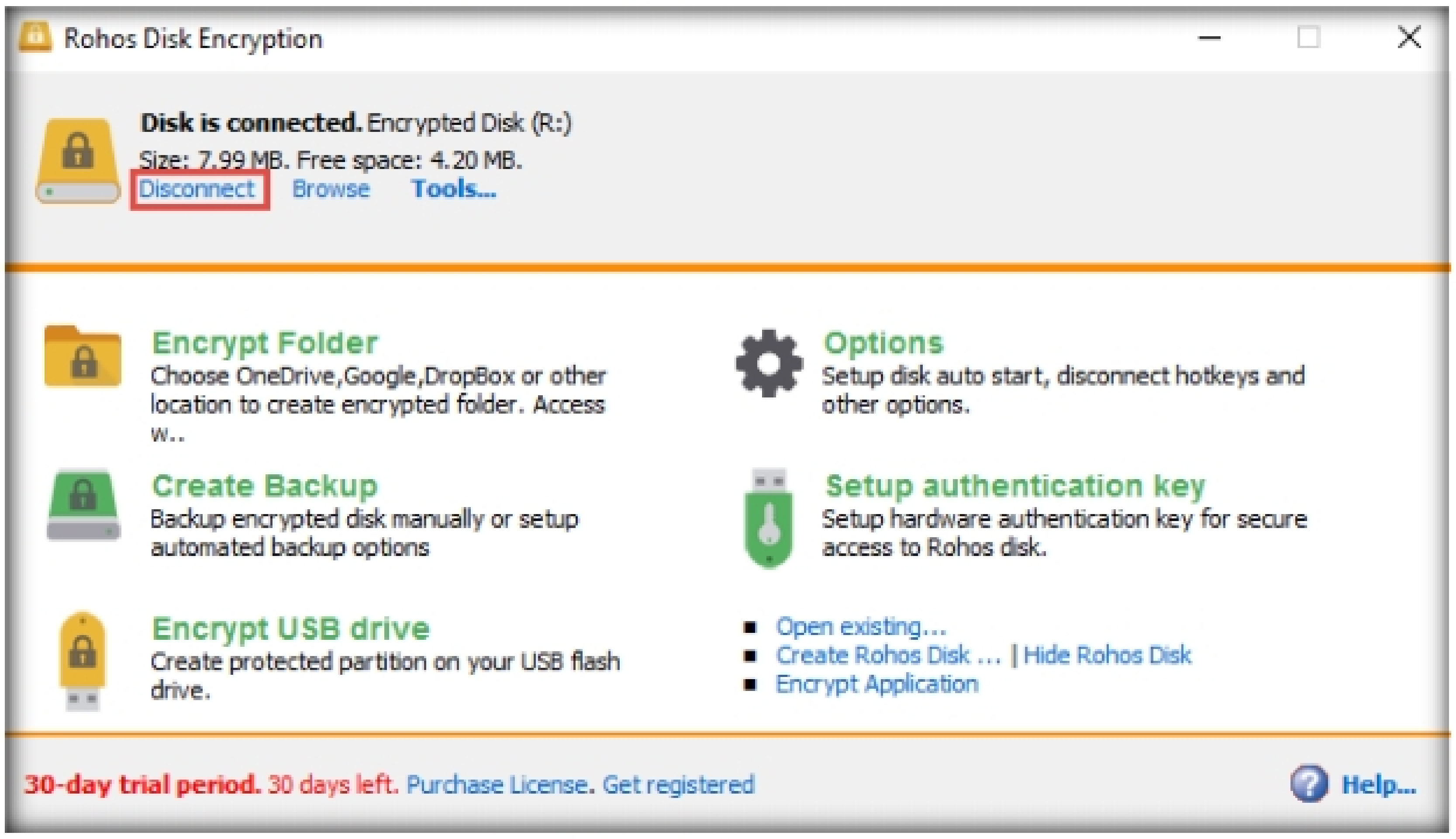
16. Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.


Encrypted Disk (R:)
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New
Properties
Open
Select
This PC › Encrypted Disk (R:)
Search Encrypted Disk (...
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Encrypted Disk (R:)
New Volume (E:)
Network
7 items
1 item selected 43 bytes

Name	Date modified
Autorun	12/12/2019 4:06 PM
Documents	12/12/2019 4:06 PM
Program Files	12/12/2019 4:06 PM
Shortcuts	12/12/2019 4:06 PM
System Volume Information	12/12/2019 4:18 PM
shares.dat	12/12/2019 4:19 PM
Test.txt	12/12/2019 4:45 PM

Figure 4.3.11: Test.txt file in Encrypted Container

17. Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.



Rohos Disk Encryption

Disk is connected. Encrypted Disk (R:)
Size: 7.99 MB. Free space: 4.20 MB.

Disconnect
Browse
Tools...

Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Options
Setup disk auto start, disconnect hotkeys and other options.

Create Backup
Backup encrypted disk manually or setup automated backup options

Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.

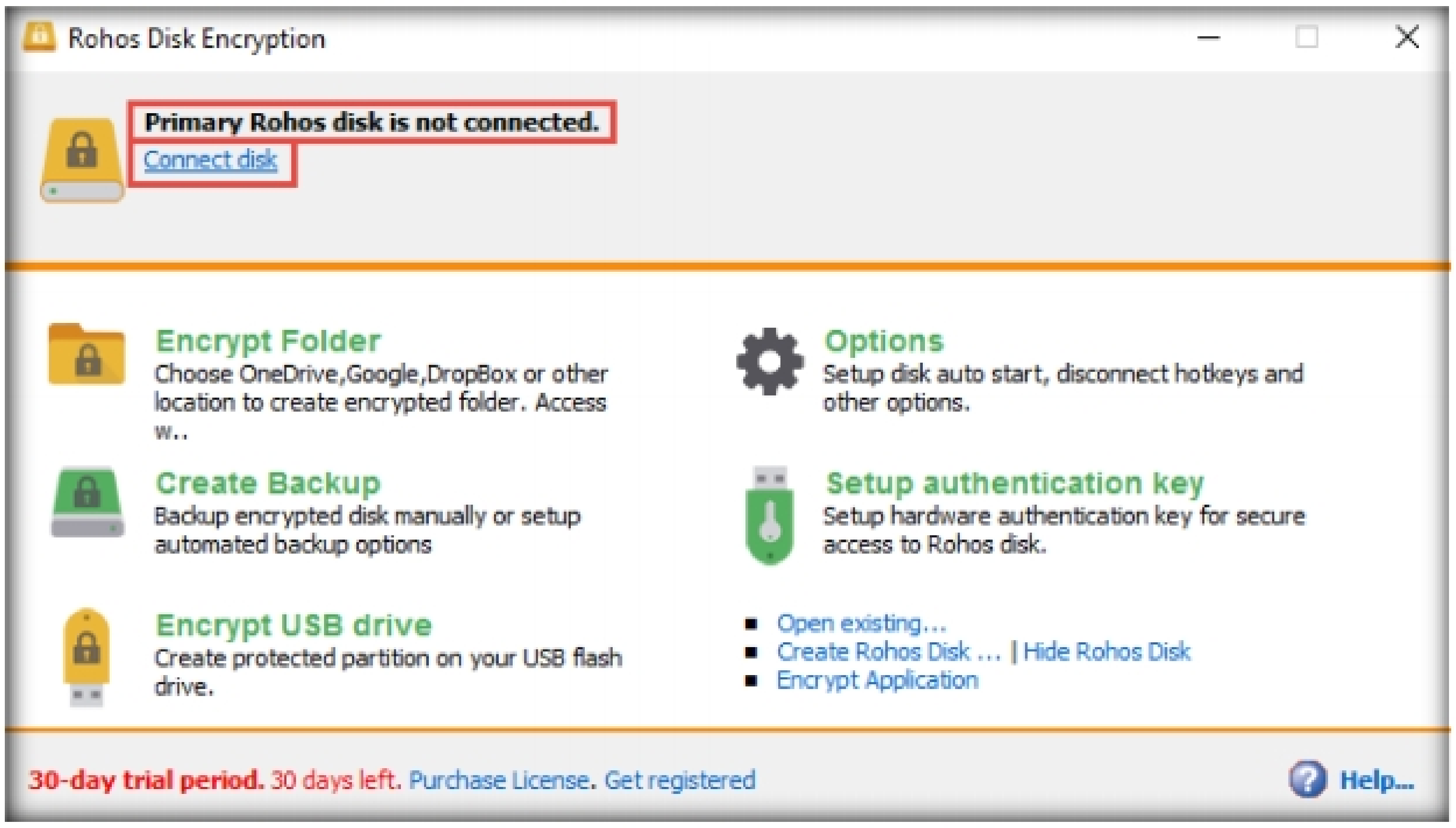
Encrypt USB drive
Create protected partition on your USB flash drive.

Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application

30-day trial period. 30 days left. Purchase License. Get registered

Figure 4.3.12: Click Disconnect to dismount

18. A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.



Rohos Disk Encryption

Primary Rohos disk is not connected.

Connect disk

Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Options
Setup disk auto start, disconnect hotkeys and other options.

Create Backup
Backup encrypted disk manually or setup automated backup options

Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.

Encrypt USB drive
Create protected partition on your USB flash drive.

Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application

30-day trial period. 30 days left. Purchase License. Get registered

Figure 4.3.13: Click Connect to mount the disk

TASK 3.4

Access Files in the Encrypted Disk

19. The **Rohos** pop-up appears; type the password you provided in **Step#9** into the **Enter password to access Rohos disk** field and click **OK**.

Note: Here, the password is **test@123**.

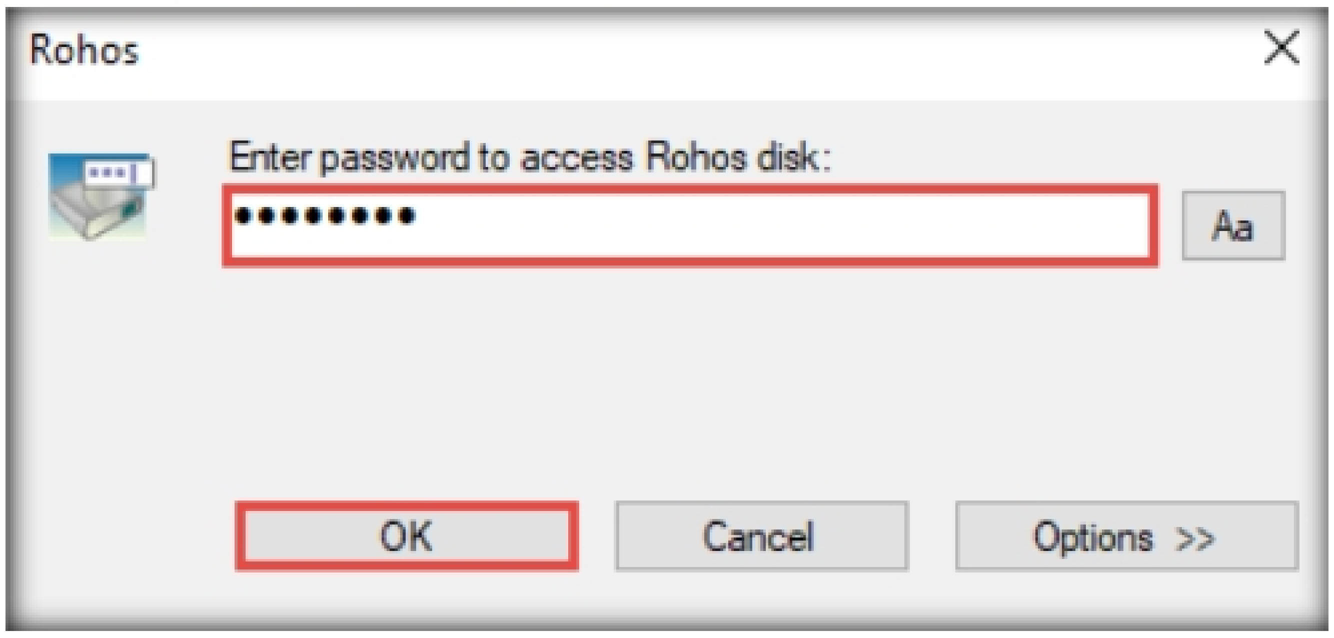

Rohos
Enter password to access Rohos disk:
••••••••
Aa
OK
Cancel
Options >>

Figure 4.3.14: Rohos pop-up

20. The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.

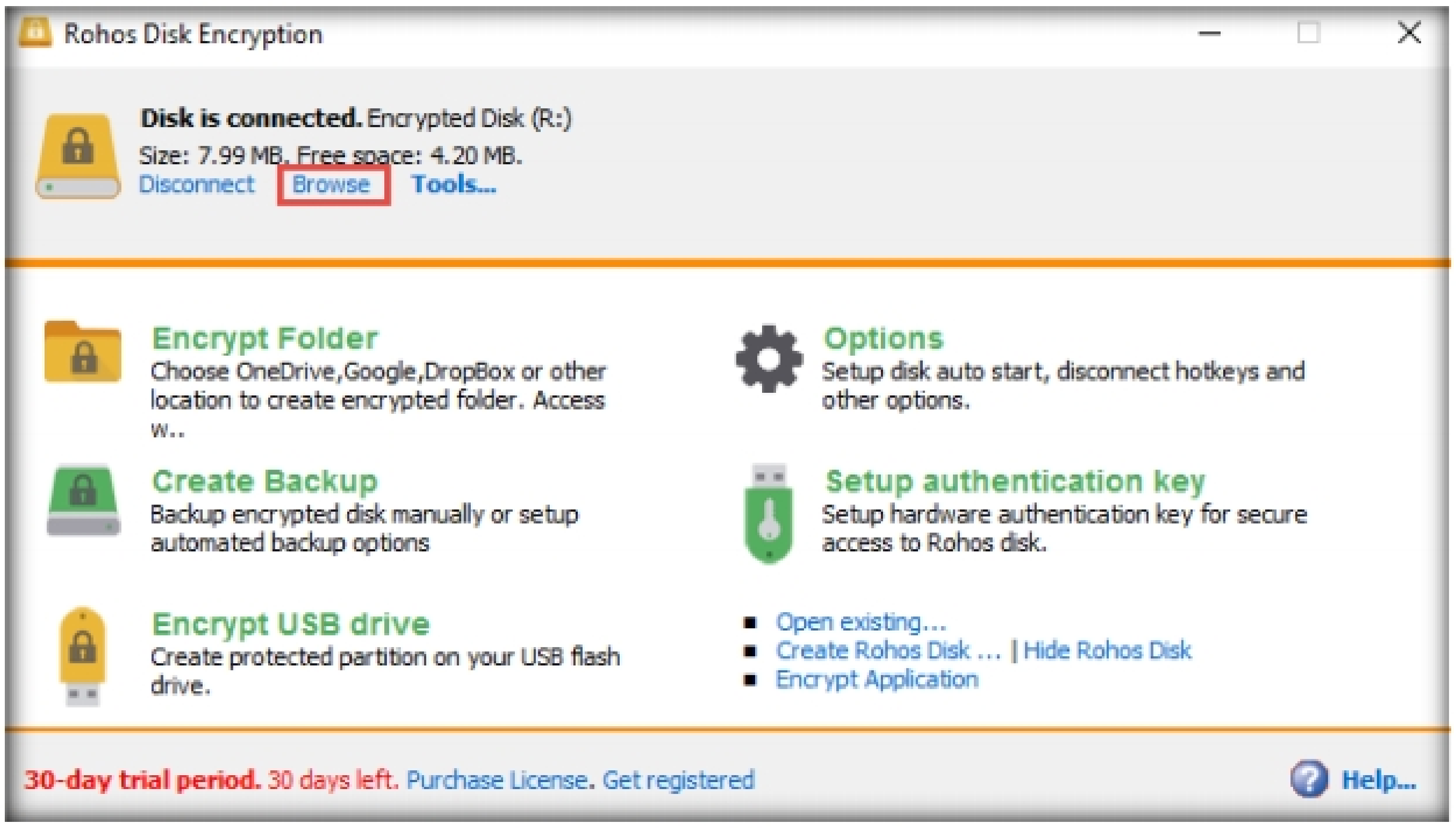
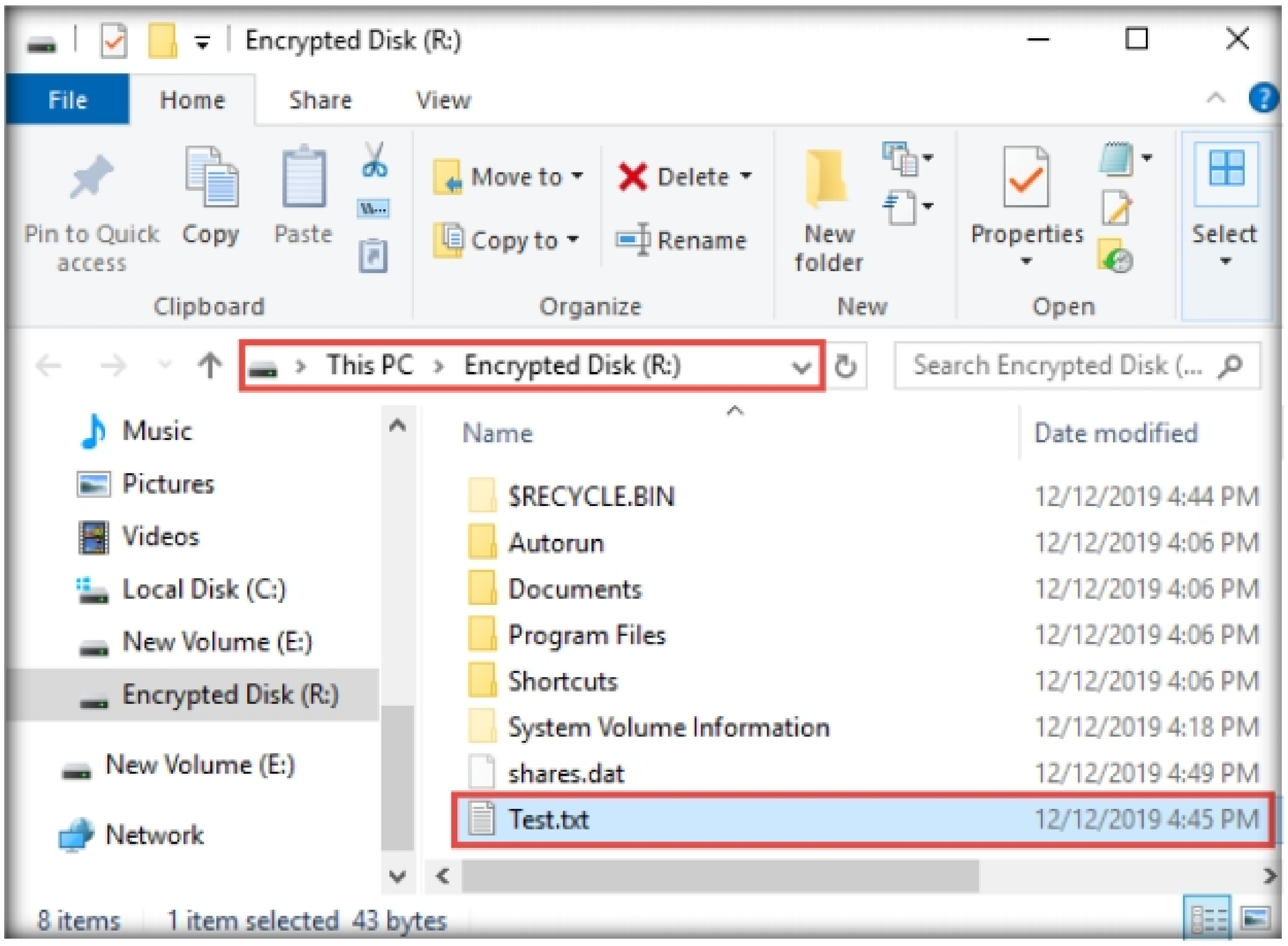

Rohos Disk Encryption
Disk is connected. Encrypted Disk (R:)
Size: 7.99 MB. Free space: 4.20 MB.
Disconnect
Browse
Tools...
Encrypt Folder
Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..
Options
Setup disk auto start, disconnect hotkeys and other options.
Create Backup
Backup encrypted disk manually or setup automated backup options
Setup authentication key
Setup hardware authentication key for secure access to Rohos disk.
Encrypt USB drive
Create protected partition on your USB flash drive.
Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application
30-day trial period. 30 days left. Purchase License. Get registered
Help...

Figure 4.3.15: Disk is connected

21. The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.


Encrypted Disk (R:)
File
Home
Share
View
Pin to Quick access
Copy
Paste
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New
Properties
Open
Select
This PC > Encrypted Disk (R:)
Search Encrypted Disk (...
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Encrypted Disk (R:)
New Volume (E:)
Network

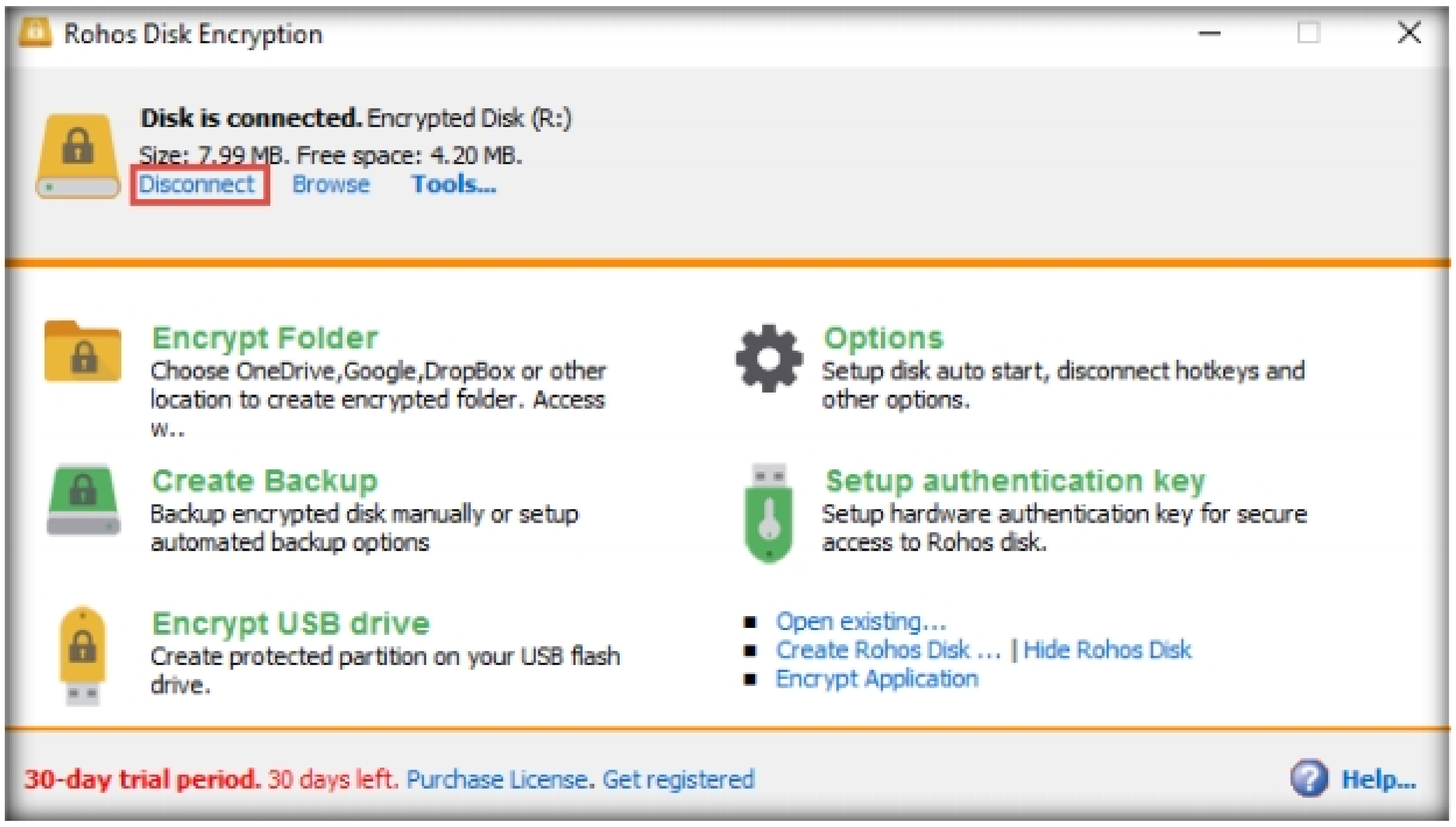
Name	Date modified
$RECYCLE.BIN	12/12/2019 4:44 PM
Autorun	12/12/2019 4:06 PM
Documents	12/12/2019 4:06 PM
Program Files	12/12/2019 4:06 PM
Shortcuts	12/12/2019 4:06 PM
System Volume Information	12/12/2019 4:18 PM
shares.dat	12/12/2019 4:49 PM
Test.txt	12/12/2019 4:45 PM

8 items | 1 item selected 43 bytes

Figure 4.3.16: Encrypted disk (R:) content

You can also use other disk encryption tools such as **FinalCrypt** (http://www.finalcrypt.org), **Seqrite Encryption Manager** (https://www.seqrite.com), **FileVault** (https://support.apple.com), and **Gillsoft Full Disk Encryption** (http://www.gilisoft.com) to perform disk encryption.

22. You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.


Rohos Disk Encryption
Disconnect
Browse
Tools...
Encrypt Folder
Options
Create Backup
Setup authentication key
Encrypt USB drive
Open existing...
Create Rohos Disk ... | Hide Rohos Disk
Encrypt Application
Help...

Disk is connected. Encrypted Disk (R:)
Size: 7.99 MB. Free space: 4.20 MB.

Choose OneDrive,Google,DropBox or other location to create encrypted folder. Access w..

Setup disk auto start, disconnect hotkeys and other options.

Backup encrypted disk manually or setup automated backup options

Setup hardware authentication key for secure access to Rohos disk.

Create protected partition on your USB flash drive.

30-day trial period. 30 days left. Purchase License. Get registered

Figure 4.3.17: Disconnect to dismount

Note: You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.
24. Close all open windows and document all the acquired information
25. Turn off **Windows 10** virtual machine.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ **Yes**	☑ **No**
Platform Supported	
☑ **Classroom**	☑ **iLabs**

Lab
5

Perform Cryptanalysis using Various Cryptanalysis Tools

Cryptanalysis is the study of ciphers, cipher text, or cryptosystems with the ability to identify vulnerabilities that allows extraction of plaintext from the ciphertext, even if the cryptographic key or algorithm used to encrypt the plaintext is unknown.

Lab Scenario

ICON KEY

🗀 Valuable information

✎ Test your knowledge

💻 Web exercise

📖 Workbook review

🗀 **Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 20 Cryptography**

Attackers tend to focus on easy to compromise targets. Therefore, in order to attain maximum network security, strong encryption is needed for all the traffic placed onto the transmission media, no matter the type and location: if an attacker wishes to break into an encrypted network, he/she faces decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to try and find another target that is easy to compromise or will simply abort the attempt. Using the latest encryption algorithms provides a strong layer of security to an organization.

As a professional ethical hacker or pen tester, you should possess the required knowledge to investigate the security of cryptographic systems. In order to confirm the security of the cryptographic systems, you must implement various cryptography attacks to evade the system's security by exploiting vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes.

In this lab, you will learn how to compromise cryptographic systems using various cryptanalysis techniques and tools that help in breaching cryptographic security.

Lab Objectives

- Perform cryptanalysis using CrypTool
- Perform cryptanalysis using AlphaPeeler

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

- Windows Server 2019 virtual machine
- Administrator privileges to run the tools
- Web browsers with an Internet connection
- CrypTool located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**
- AlphaPeeler located at **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest versions, the screenshots shown in the lab might differ.

Lab Duration

Time: 25 Minutes

Overview of Cryptanalysis

Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis**: A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis**: The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis**: This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

Lab Tasks

TASK 1

Perform Cryptanalysis using CrypTool

Here, we will use the CrypTool tool to perform cryptanalysis.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

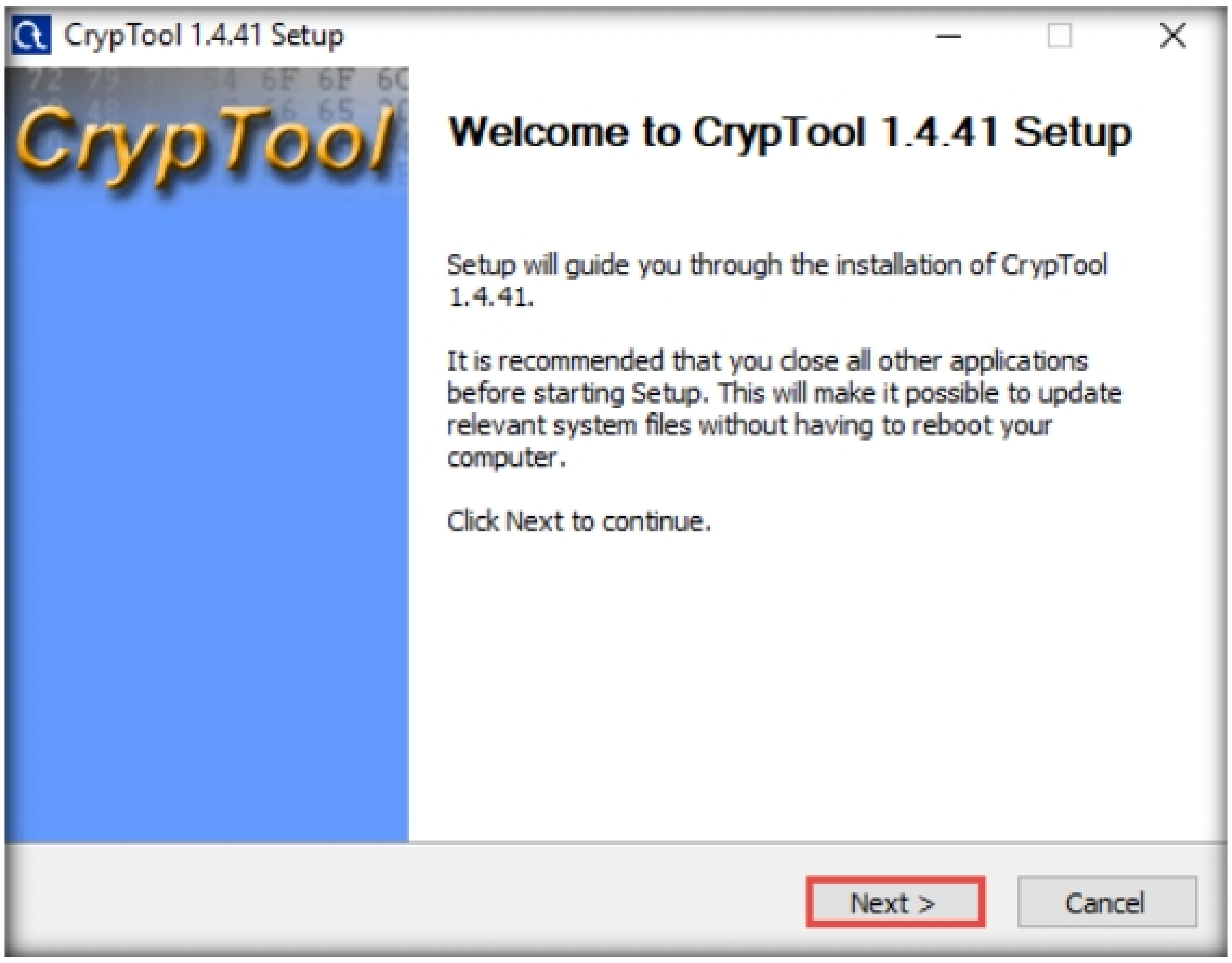
Install and Launch CrypTool

3. Navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and double-click **SetupCrypTool_1_4_41_en.exe**.

Note: If a **User Account Control** pop-up appears, click **Yes**.

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

4. The **CrypTool Setup** window appears; then, click **Next**.



CrypTool 1.4.41 Setup

Welcome to CrypTool 1.4.41 Setup

Setup will guide you through the installation of CrypTool 1.4.41.

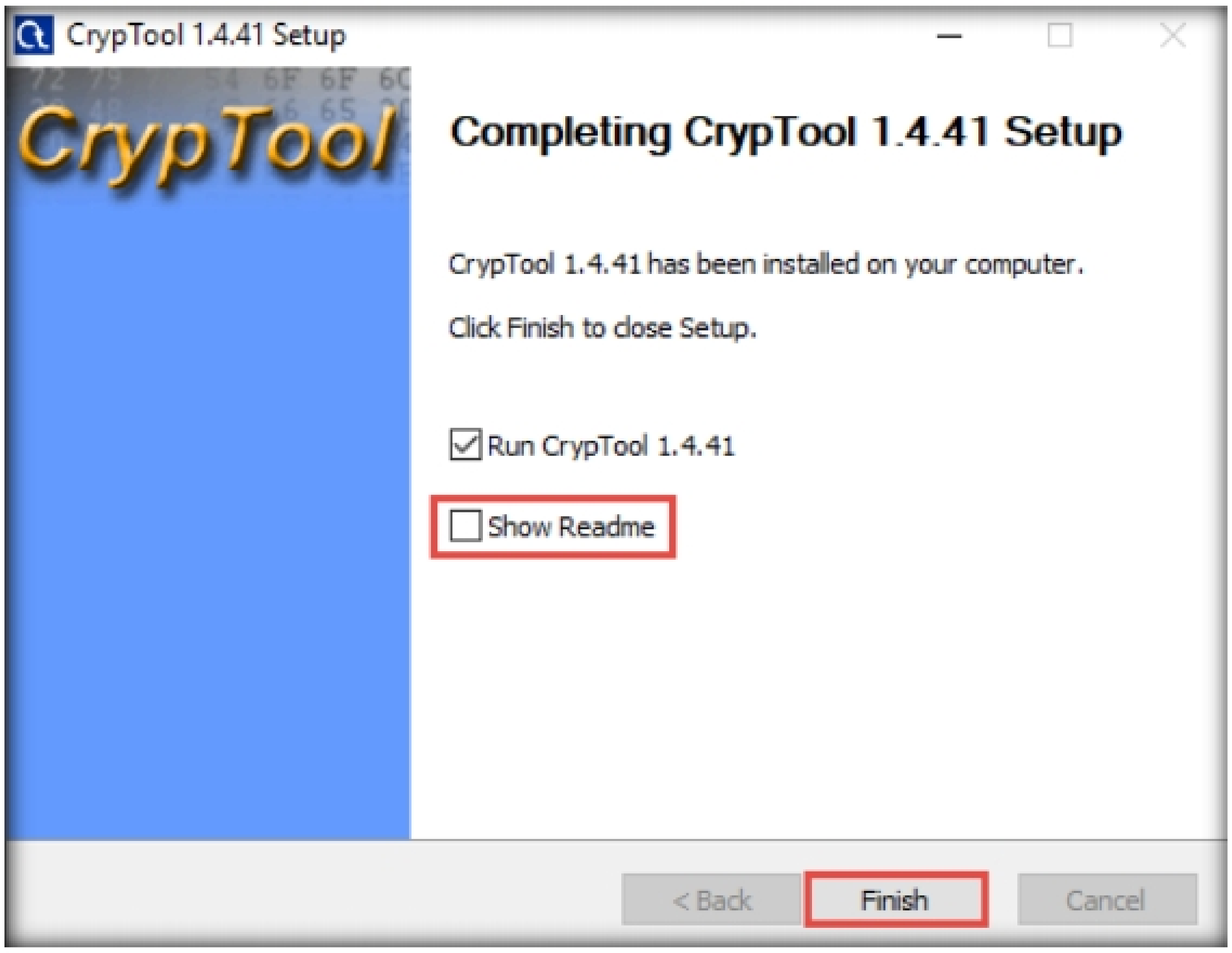
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 5.1.1: CrypTool Setup window

5. Follow the wizard-driven installation steps to install the application using all default settings.

6. After the completion of the installation, the **Completing CrypTool Setup** wizard appears; uncheck the **Show Readme** checkbox and click **Finish**.



CrypTool 1.4.41 Setup

Completing CrypTool 1.4.41 Setup

CrypTool 1.4.41 has been installed on your computer.

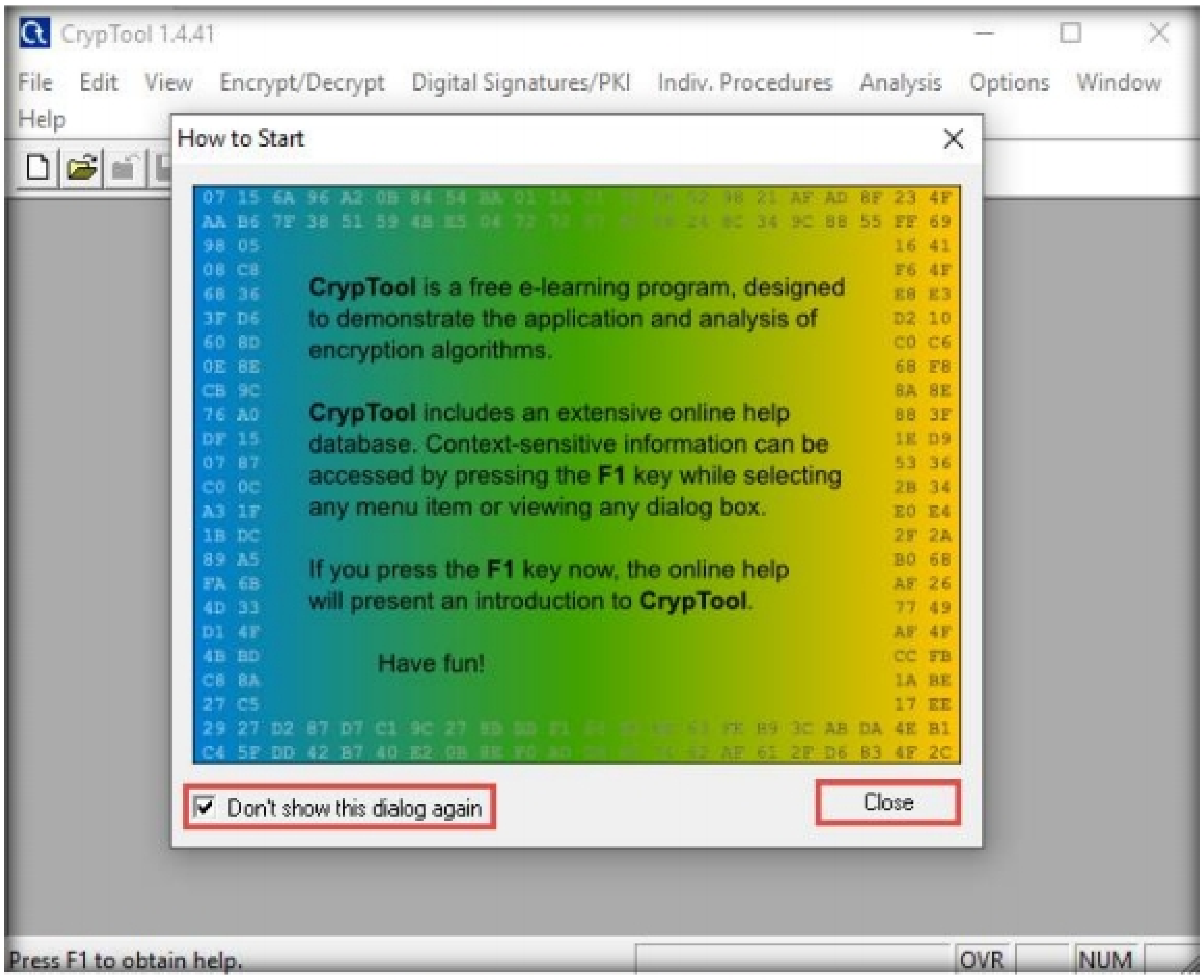
Click Finish to close Setup.

☑ Run CrypTool 1.4.41

☐ Show Readme

Figure 5.1.2: Completing CrypTool Setup window

7. The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.


CrypTool 1.4.41
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
How to Start
☑ Don't show this dialog again
Close
Press F1 to obtain help.
OVR
NUM

CrypTool is a free e-learning program, designed to demonstrate the application and analysis of encryption algorithms.

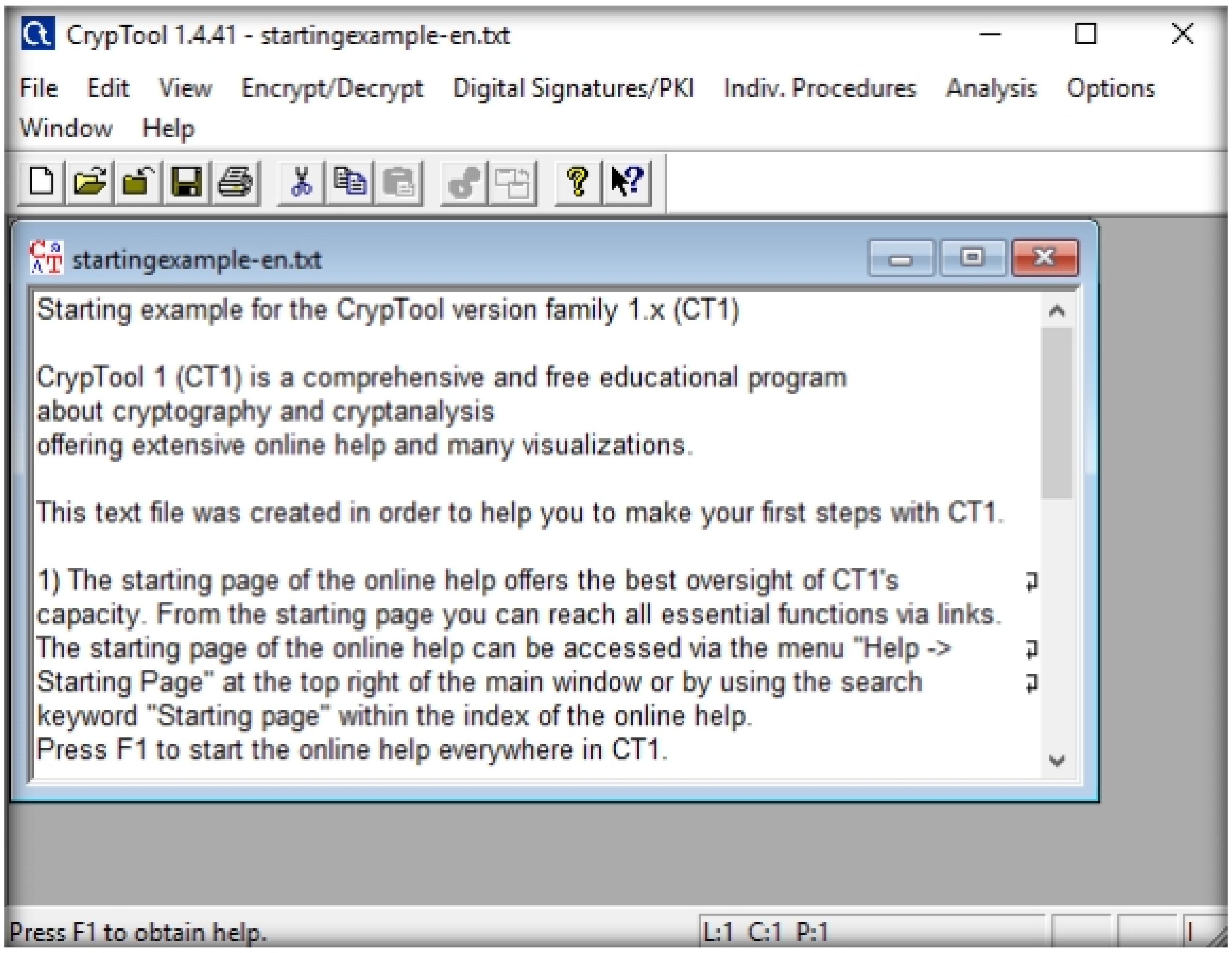
CrypTool includes an extensive online help database. Context-sensitive information can be accessed by pressing the **F1** key while selecting any menu item or viewing any dialog box.

If you press the **F1** key now, the online help will present an introduction to **CrypTool**.

Have fun!

Figure 5.1.3: How to Start Dialog box

8. The **CrypTool** window appears; close the **startingexample-en.txt** window.


CrypTool 1.4.41 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
Press F1 to obtain help.
L:1 C:1 P:1

Starting example for the CrypTool version family 1.x (CT1)

CrypTool 1 (CT1) is a comprehensive and free educational program
about cryptography and cryptanalysis
offering extensive online help and many visualizations.

This text file was created in order to help you to make your first steps with CT1.

1) The starting page of the online help offers the best oversight of CT1's
capacity. From the starting page you can reach all essential functions via links.
The starting page of the online help can be accessed via the menu "Help ->
Starting Page" at the top right of the main window or by using the search
keyword "Starting page" within the index of the online help.
Press F1 to start the online help everywhere in CT1.

Figure 5.1.4: startingexample-en.txt window in CrypTool

9. Click the **File** option from the menu bar and select **New** to create encrypted data.

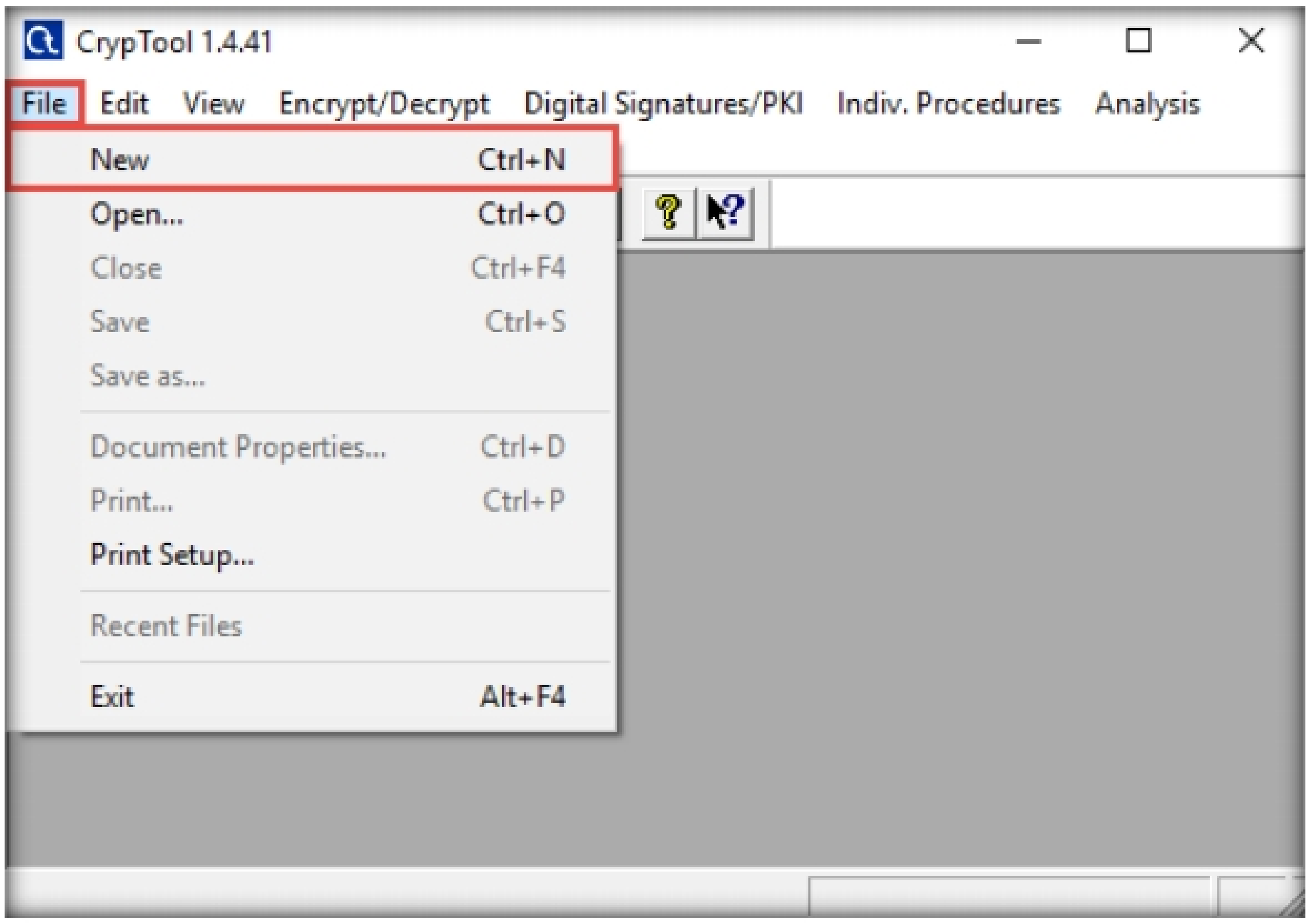

CrypTool 1.4.41
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
New Ctrl+N
Open... Ctrl+O
Close Ctrl+F4
Save Ctrl+S
Save as...
Document Properties... Ctrl+D
Print... Ctrl+P
Print Setup...
Recent Files
Exit Alt+F4

Figure 5.1.5: Choosing a new file to crypt

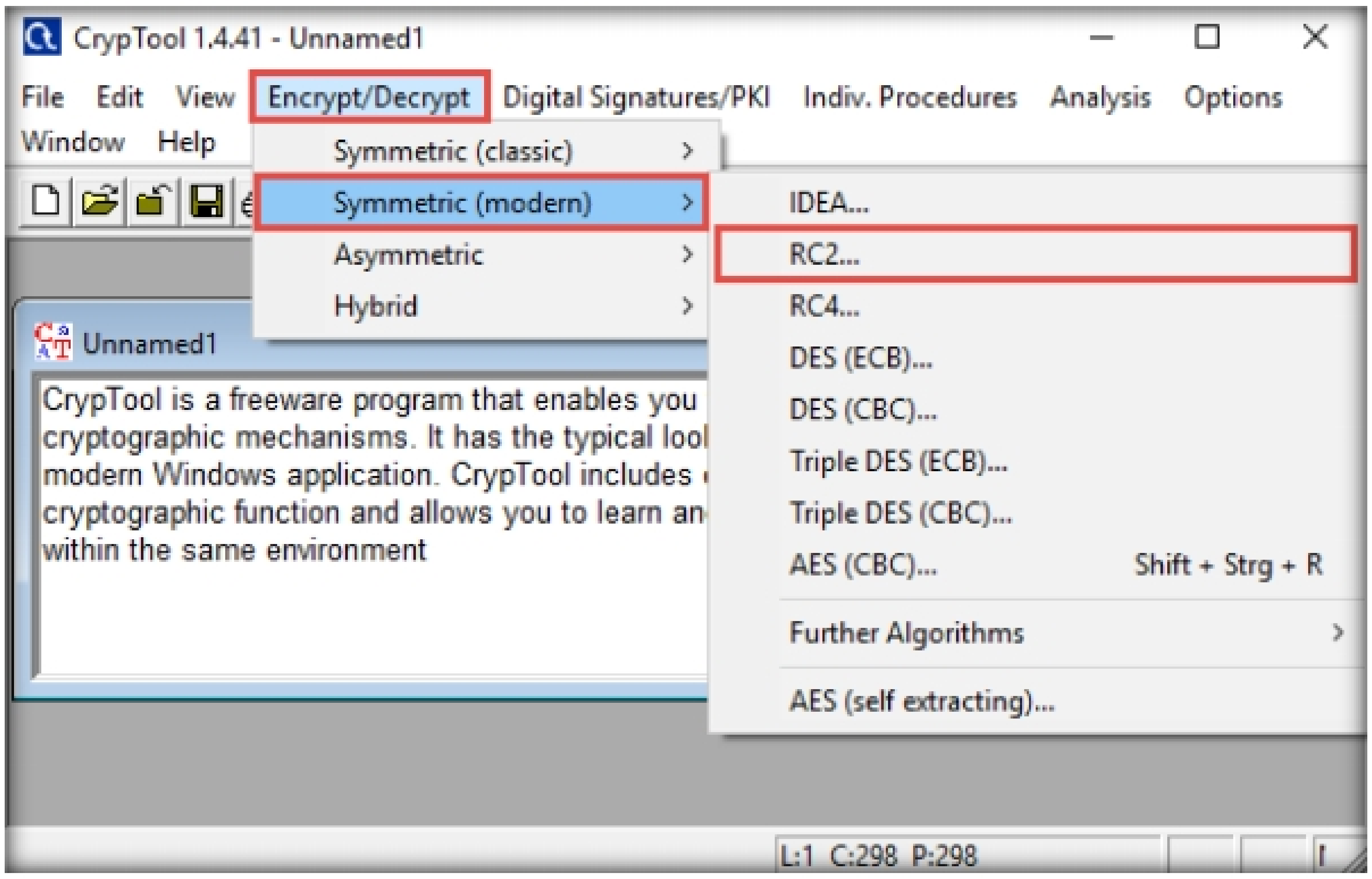
10. The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.

TASK 1.2

Encrypt the Data using RC2 Encryption

11. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**.

Note: RC2 is a symmetric-key block cipher. It is a 64-bit block cipher with variable key size and uses 18 rounds.


CrypTool 1.4.41 - Unnamed1
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)... Shift + Strg + R
Further Algorithms
AES (self extracting)...
Unnamed1
L:1 C:298 P:298

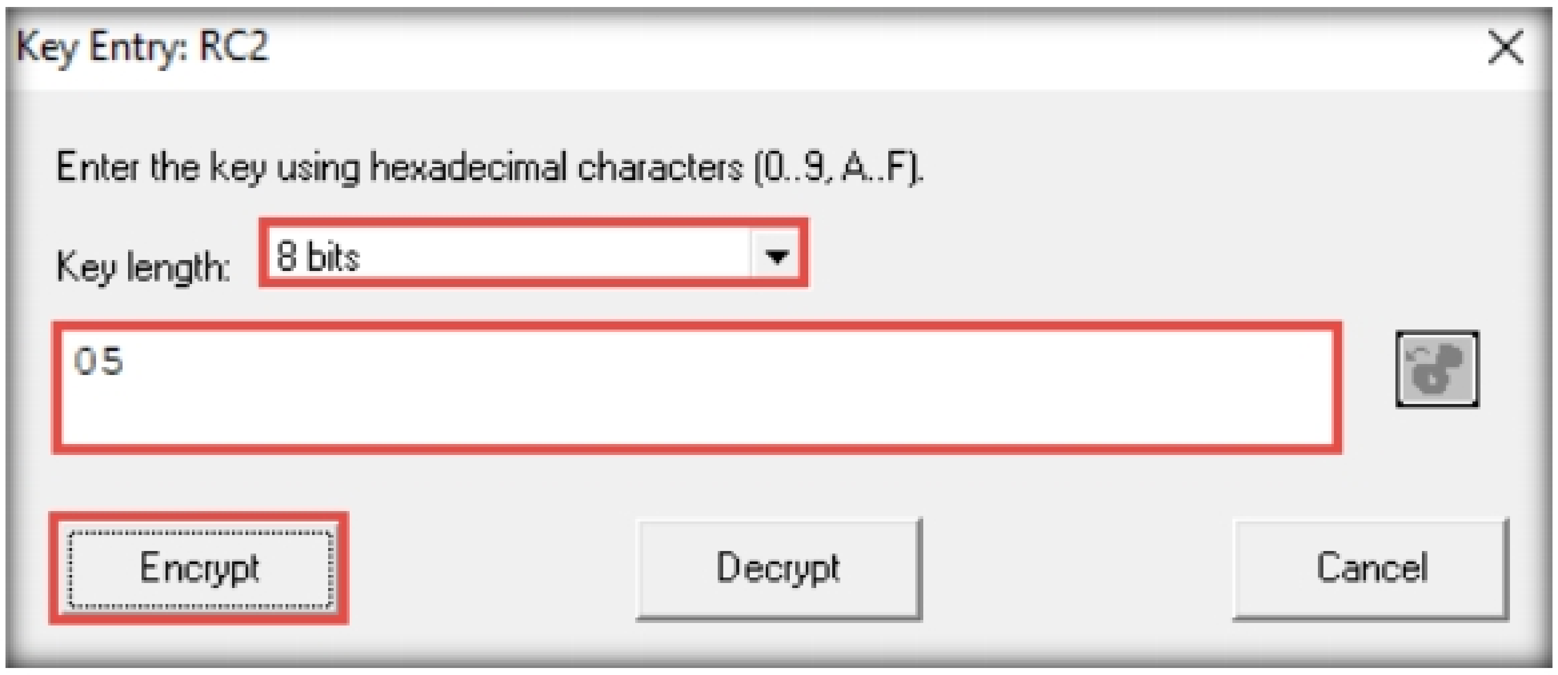
CrypTool is a freeware program that enables you
cryptographic mechanisms. It has the typical lool
modern Windows application. CrypTool includes
cryptographic function and allows you to learn an
within the same environment

Figure 5.1.6: Encrypting the file

12. The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).

13. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.



Key Entry: RC2

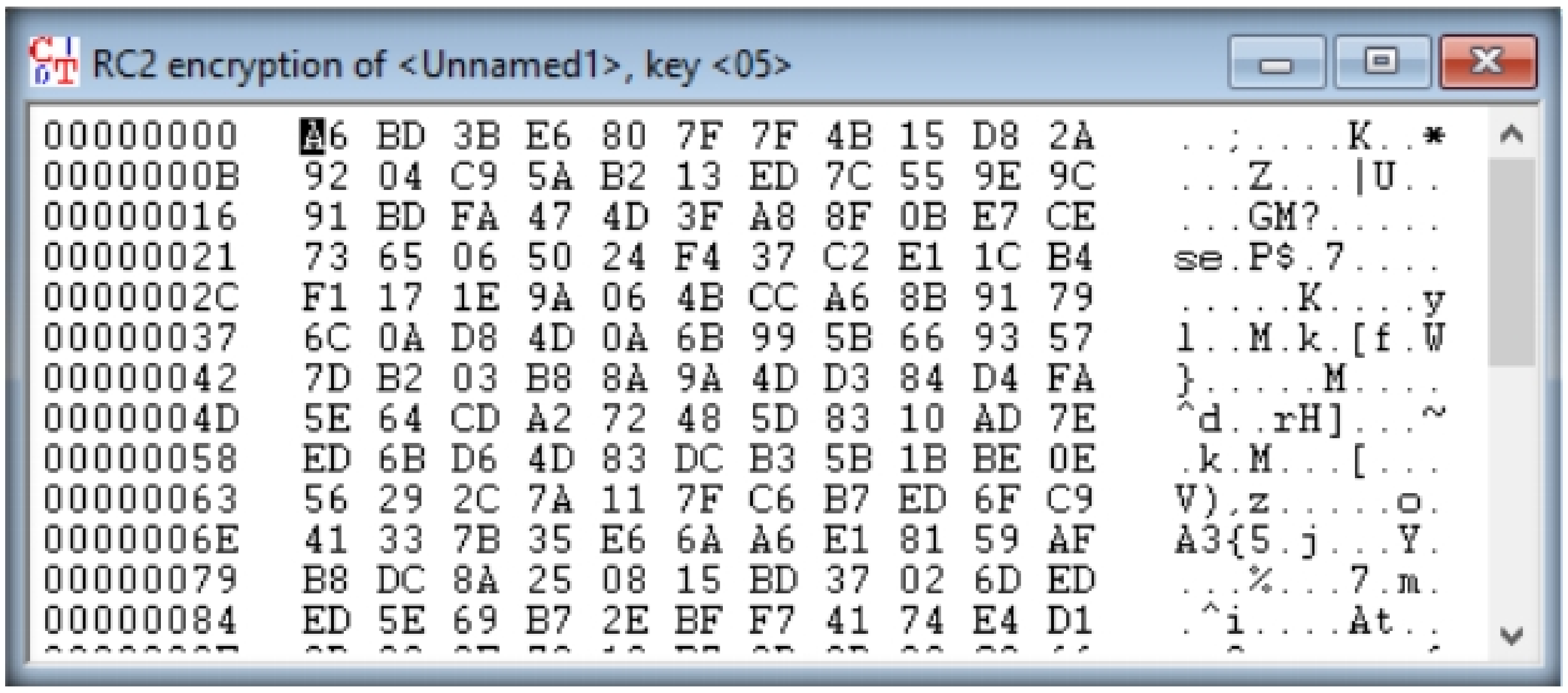
Enter the key using hexadecimal characters (0..9, A..F).

Key length: 8 bits

05

Figure 5.1.7: Encrypting the file

14. The **RC encryption of Unnamed1** notepad file appears, as shown in the screenshot.



RC2 encryption of <Unnamed1>, key <05>

```
00000000   A6 BD 3B E6 80 7F 7F 4B 15 D8 2A    ..;....K..*
0000000B   92 04 C9 5A B2 13 ED 7C 55 9E 9C    ...Z...|U..
00000016   91 BD FA 47 4D 3F A8 8F 0B E7 CE    ...GM?.....
00000021   73 65 06 50 24 F4 37 C2 E1 1C B4    se.P$.7....
0000002C   F1 17 1E 9A 06 4B CC A6 8B 91 79    .....K....y
00000037   6C 0A D8 4D 0A 6B 99 5B 66 93 57    l..M.k.[f.W
00000042   7D B2 03 B8 8A 9A 4D D3 84 D4 FA    }.....M....
0000004D   5E 64 CD A2 72 48 5D 83 10 AD 7E    ^d..rH]...~
00000058   ED 6B D6 4D 83 DC B3 5B 1B BE 0E    .k.M...[...
00000063   56 29 2C 7A 11 7F C6 B7 ED 6F C9    V),z.....o.
0000006E   41 33 7B 35 E6 6A A6 E1 81 59 AF    A3{5.j...Y.
00000079   B8 DC 8A 25 08 15 BD 37 02 6D ED    ...%...7.m.
00000084   ED 5E 69 B7 2E BF F7 41 74 E4 D1    .^i....At..
```

Figure 5.1.8: Output of RC2: encrypted data

15. To save, click **File** in the menu bar and select **Save**.

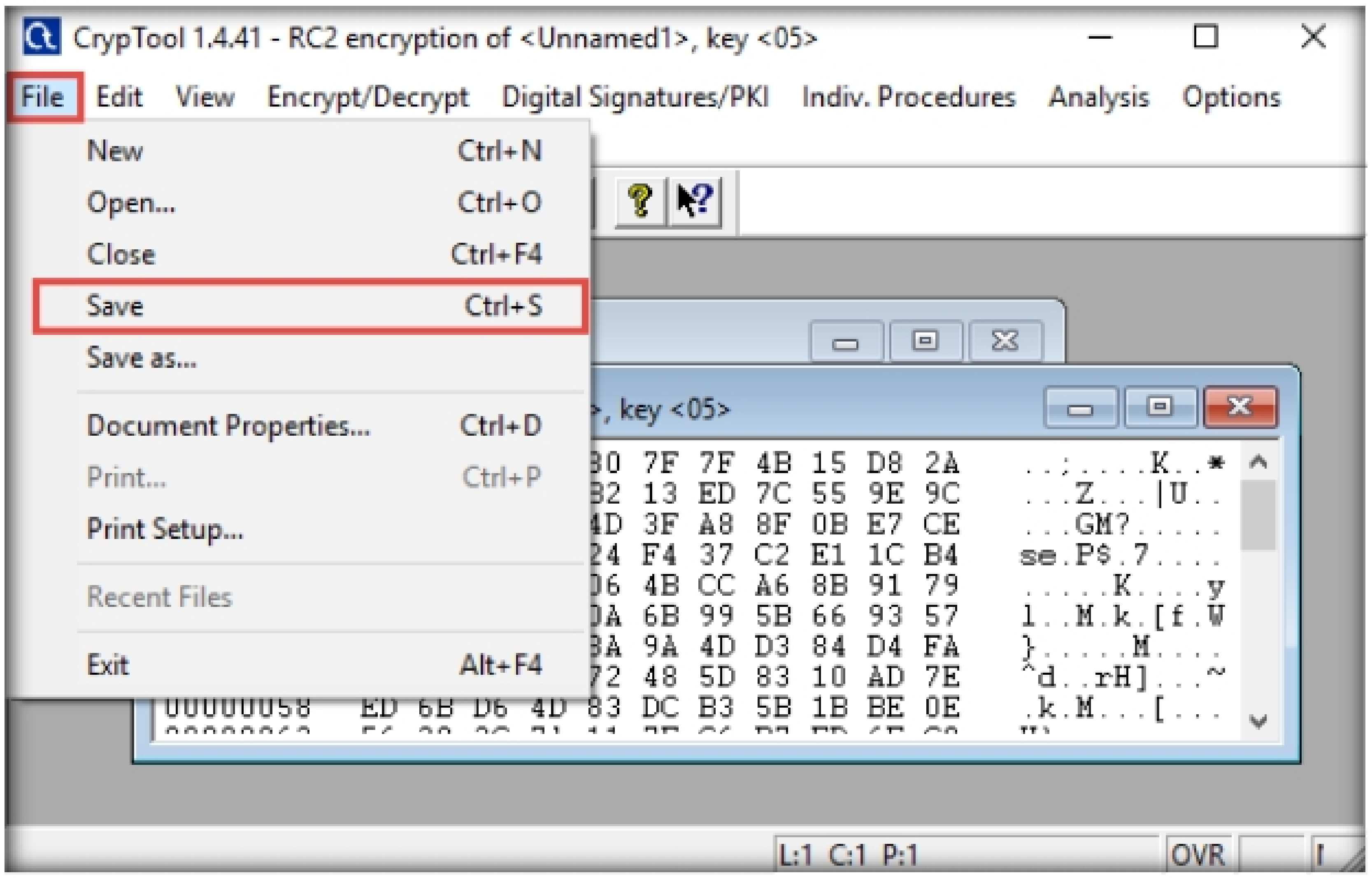
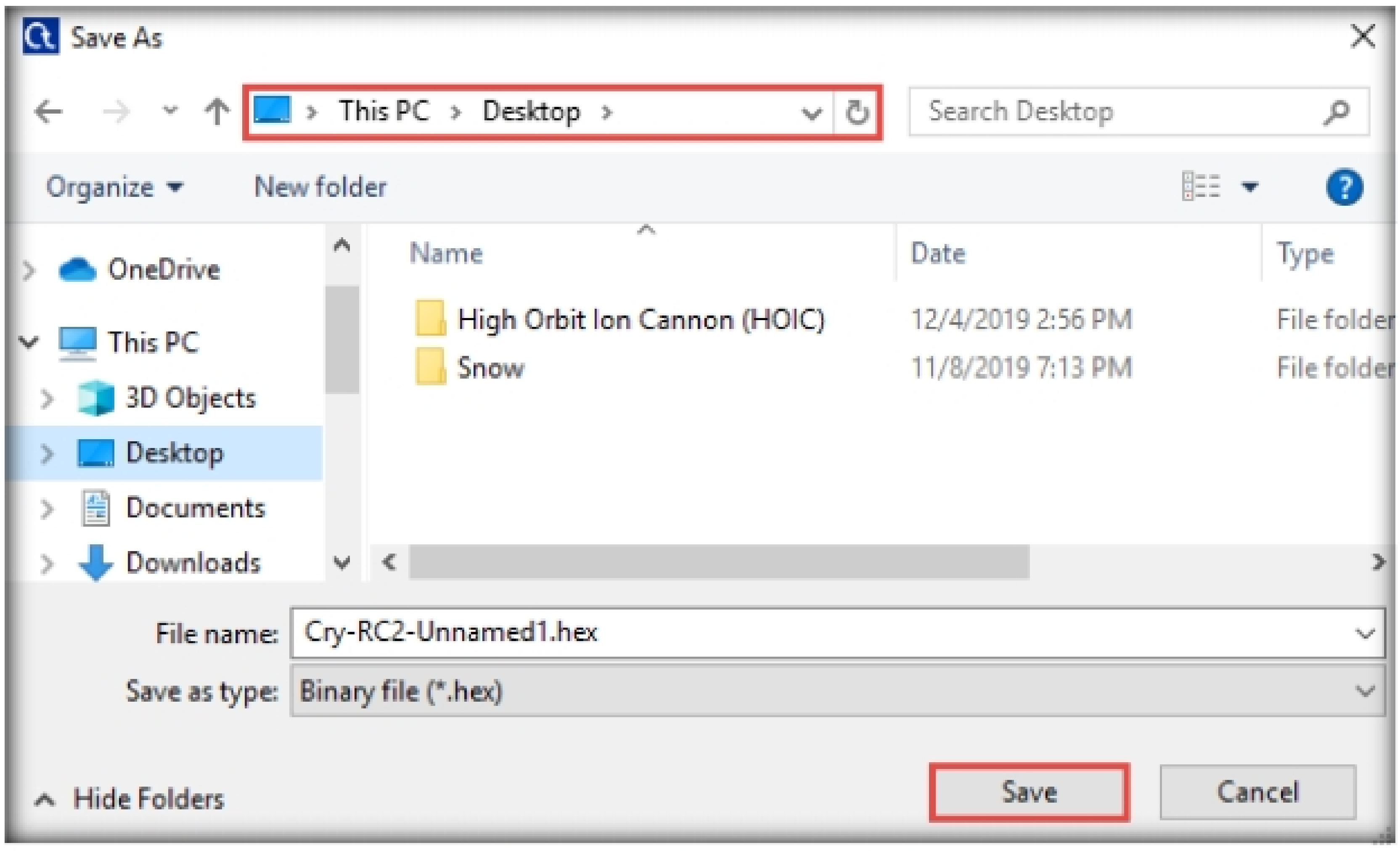

CrypTool 1.4.41 - RC2 encryption of <Unnamed1>, key <05>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
New Ctrl+N
Open... Ctrl+O
Close Ctrl+F4
Save Ctrl+S
Save as...
Document Properties... Ctrl+D
Print... Ctrl+P
Print Setup...
Recent Files
Exit Alt+F4
, key <05>
L:1 C:1 P:1
OVR

Figure 5.1.9: Saving the encrypted file

16. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.


Save As
This PC › Desktop ›
Search Desktop
Organize
New folder
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Name
Date
Type
Hide Folders
Save
Cancel

Name	Date	Type
High Orbit Ion Cannon (HOIC)	12/4/2019 2:56 PM	File folder
Snow	11/8/2019 7:13 PM	File folder

File name: Cry-RC2-Unnamed1.hex

Save as type: Binary file (*.hex)

Figure 5.1.10: Saving the encrypted file

17. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.

18. To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.

19. Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.

TASK 1.3

Decrypt the Data

20. Switch to **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.

21. Navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**, double-click **SetupCrypTool_1_4_41_en.exe**, and follow the steps to install the application using all default settings.

22. After the installation finishes, launch the **CrypTool** application.

Note: In the **How to Start** dialog-box; check **Don't show this dialog again** and click **Close**.

23. The **CrypTool** main window appears; close the **startingexample-en.txt** window.

24. Now, copy the encrypted hex file (**Cry-RC2-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste it on **Desktop**.

25. Switch to the **CrypTool** window; click **File** in the menu bar and select **Open...**

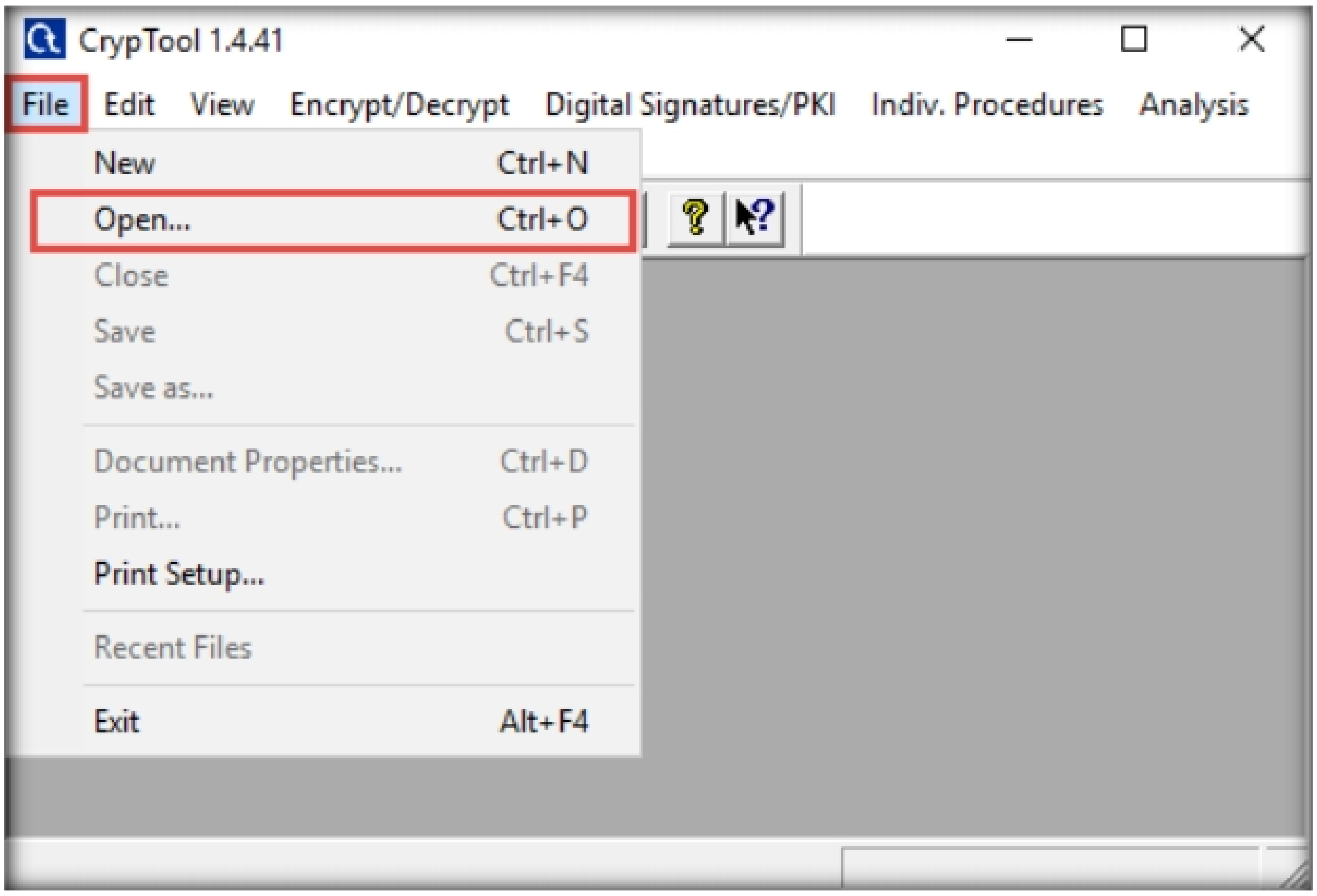

CrypTool 1.4.41
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
New Ctrl+N
Open... Ctrl+O
Close Ctrl+F4
Save Ctrl+S
Save as...
Document Properties... Ctrl+D
Print... Ctrl+P
Print Setup...
Recent Files
Exit Alt+F4

Figure 5.1.11: Opening an encrypted file

26. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.

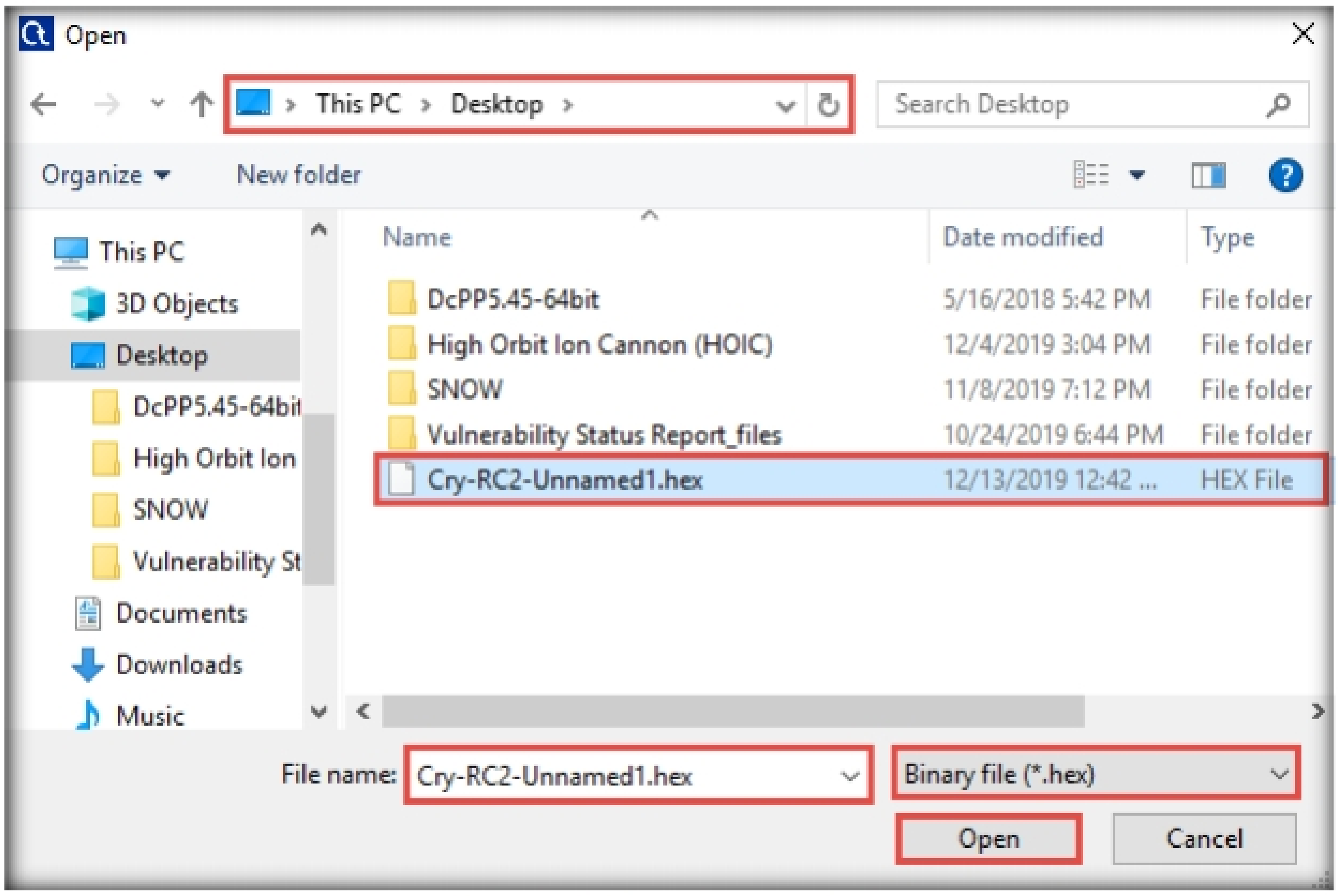
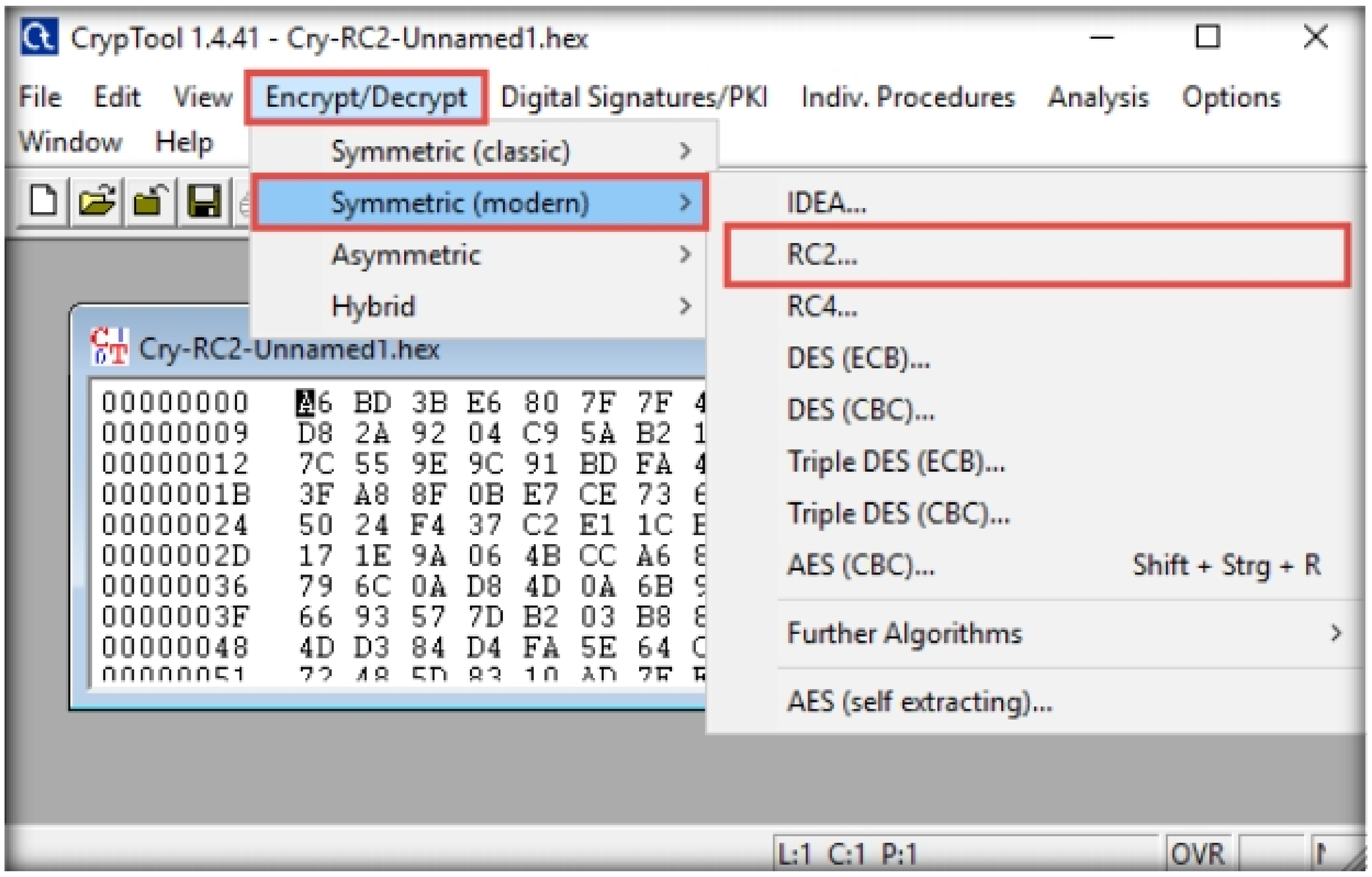

Open
This PC > Desktop >
Search Desktop
Organize ▾
New folder
This PC
3D Objects
Desktop
DcPP5.45-64bit
High Orbit Ion
SNOW
Vulnerability St
Documents
Downloads
Music
Name
Date modified
Type
DcPP5.45-64bit 5/16/2018 5:42 PM File folder
High Orbit Ion Cannon (HOIC) 12/4/2019 3:04 PM File folder
SNOW 11/8/2019 7:12 PM File folder
Vulnerability Status Report_files 10/24/2019 6:44 PM File folder
Cry-RC2-Unnamed1.hex 12/13/2019 12:42 ... HEX File
File name: Cry-RC2-Unnamed1.hex
Binary file (*.hex)
Open
Cancel

Figure 5.1.12: Opening a Crypted file

27. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → RC2...**

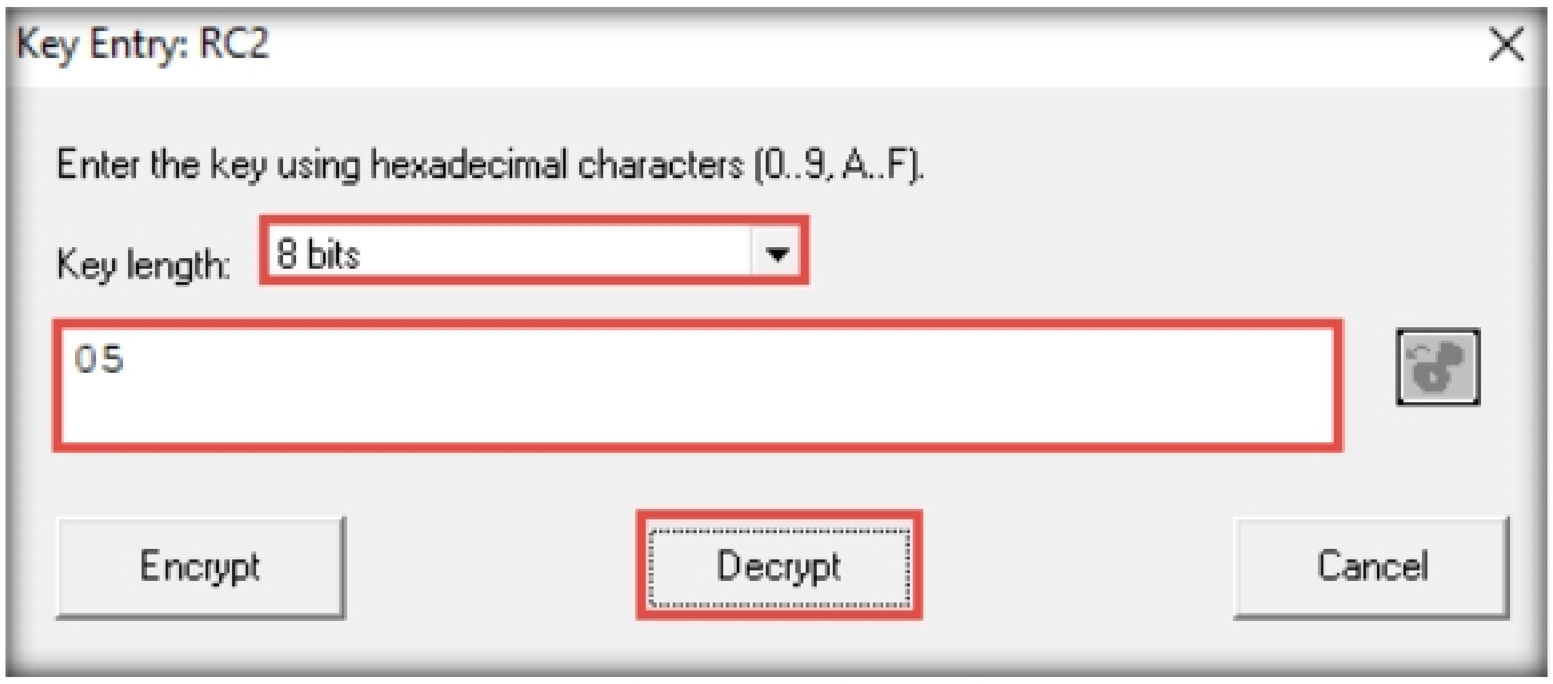

CrypTool 1.4.41 - Cry-RC2-Unnamed1.hex
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Symmetric (classic) >
Symmetric (modern) >
Asymmetric >
Hybrid >
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)... Shift + Strg + R
Further Algorithms >
AES (self extracting)...
Cry-RC2-Unnamed1.hex
L:1 C:1 P:1
OVR

```
00000000  A6 BD 3B E6 80 7F 7F 4
00000009  D8 2A 92 04 C9 5A B2 1
00000012  7C 55 9E 9C 91 BD FA 4
0000001B  3F A8 8F 0B E7 CE 73 6
00000024  50 24 F4 37 C2 E1 1C E
0000002D  17 1E 9A 06 4B CC A6 8
00000036  79 6C 0A D8 4D 0A 6B 9
0000003F  66 93 57 7D B2 03 B8 8
00000048  4D D3 84 D4 FA 5E 64 C
```

Figure 5.1.13: Select the RC2 Encryption algorithm

28. The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).

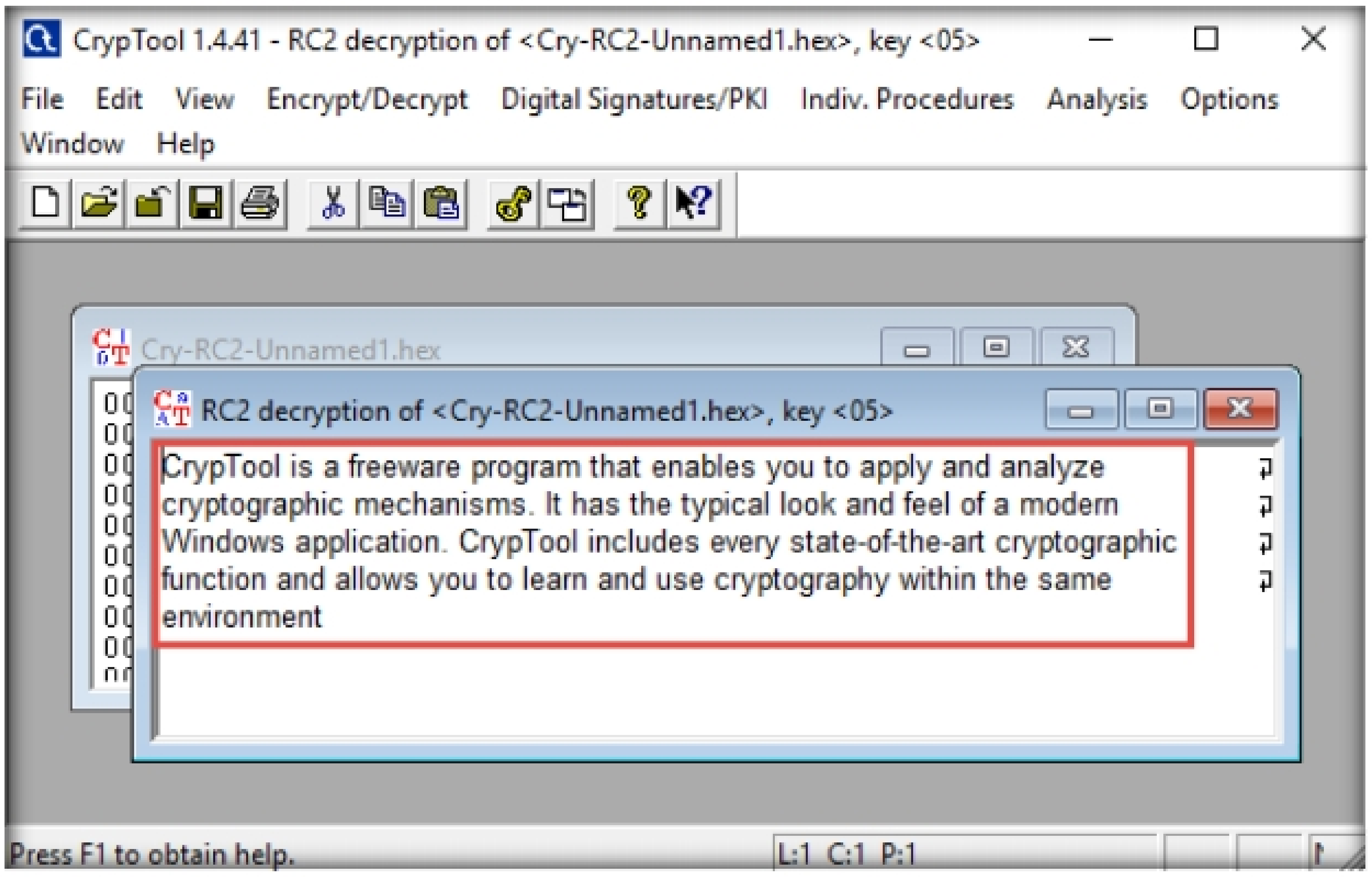
29. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.



Key Entry: RC2
Enter the key using hexadecimal characters (0..9, A..F).
Key length:
8 bits
05
Encrypt
Decrypt
Cancel

Figure 5.1.14: Decrypting the file

30. The decrypted text appears, as shown in the screenshot:



CrypTool 1.4.41 - RC2 decryption of <Cry-RC2-Unnamed1.hex>, key <05>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Cry-RC2-Unnamed1.hex
RC2 decryption of <Cry-RC2-Unnamed1.hex>, key <05>
Press F1 to obtain help.
L:1 C:1 P:1

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms. It has the typical look and feel of a modern Windows application. CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment

Figure 5.1.15: Decrypted the file successfully

31. Now, we shall encrypt the data using Triple DES encryption.

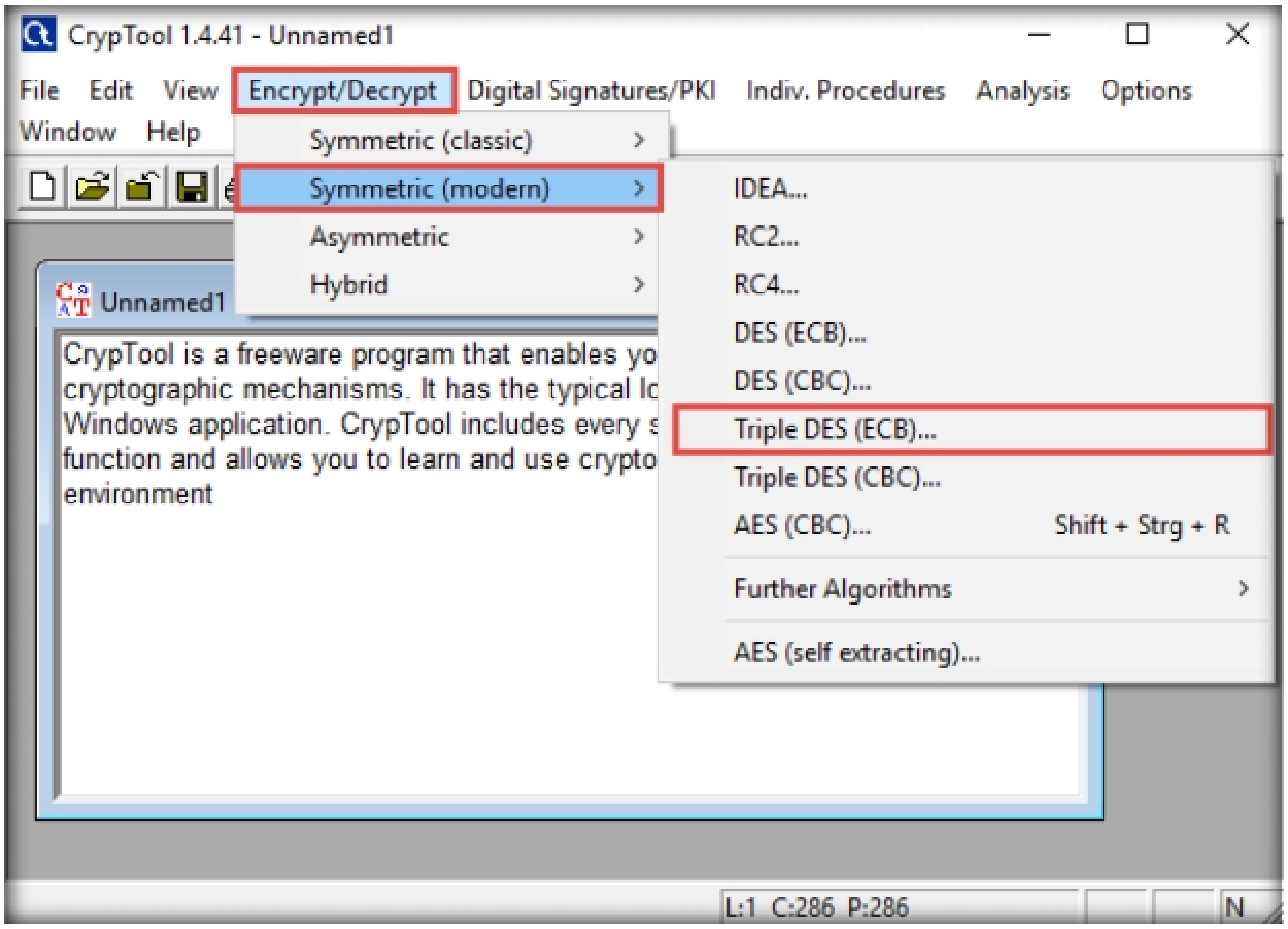
32. Switch back to the **Windows 10** virtual machine.

TASK 1.4

Encrypt the Data using Triple DES Encryption

33. In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.

34. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**


CrypTool 1.4.41 - Unnamed1
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options
Window Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)... Shift + Strg + R
Further Algorithms
AES (self extracting)...
Unnamed1
L:1 C:286 P:286 N

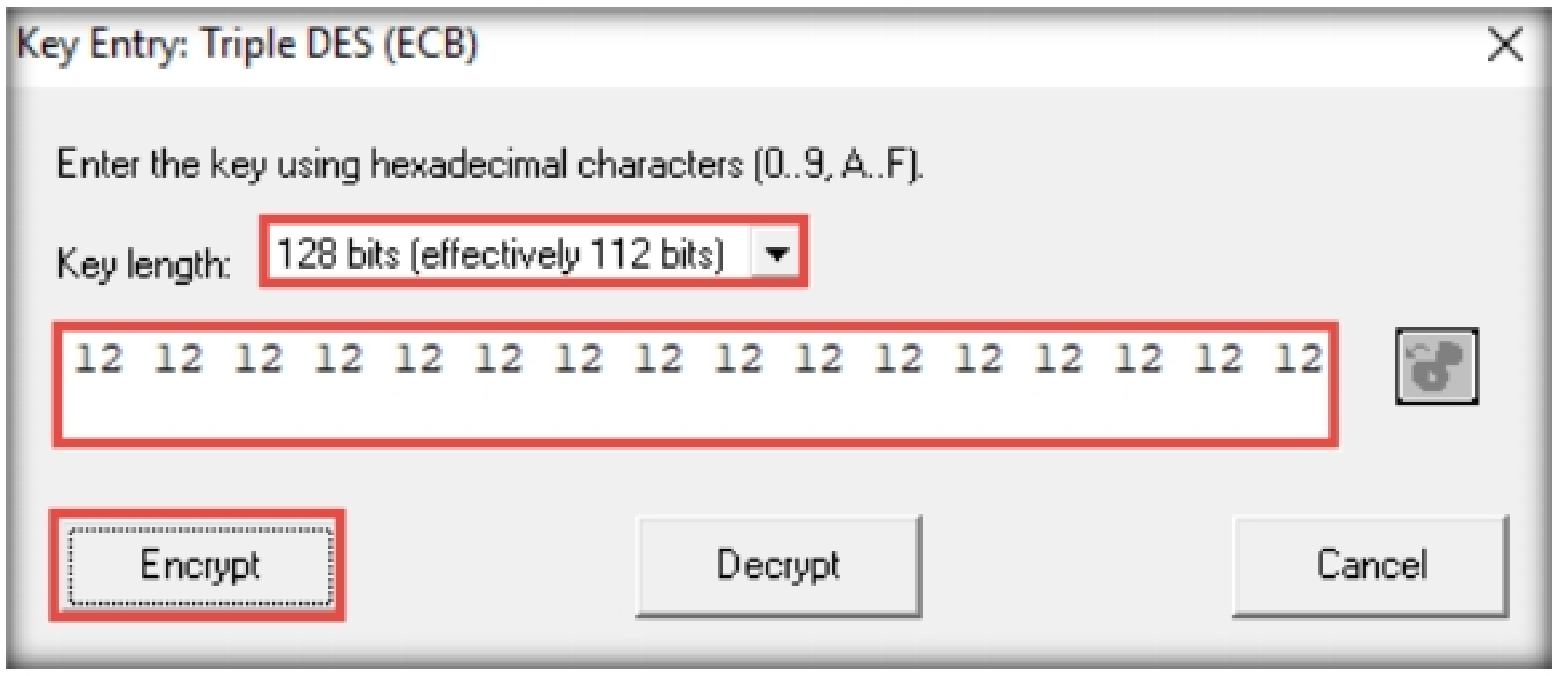
CrypTool is a freeware program that enables yo
cryptographic mechanisms. It has the typical lo
Windows application. CrypTool includes every s
function and allows you to learn and use crypto
environment

Figure 5.1.16: Select the Triple DES (ECB) Encryption algorithm

35. The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).

36. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

Note: The chosen hexadecimal characters act like a key that you must send to the intended user along with the encrypted file.


Key Entry: Triple DES (ECB)
Encrypt
Decrypt
Cancel

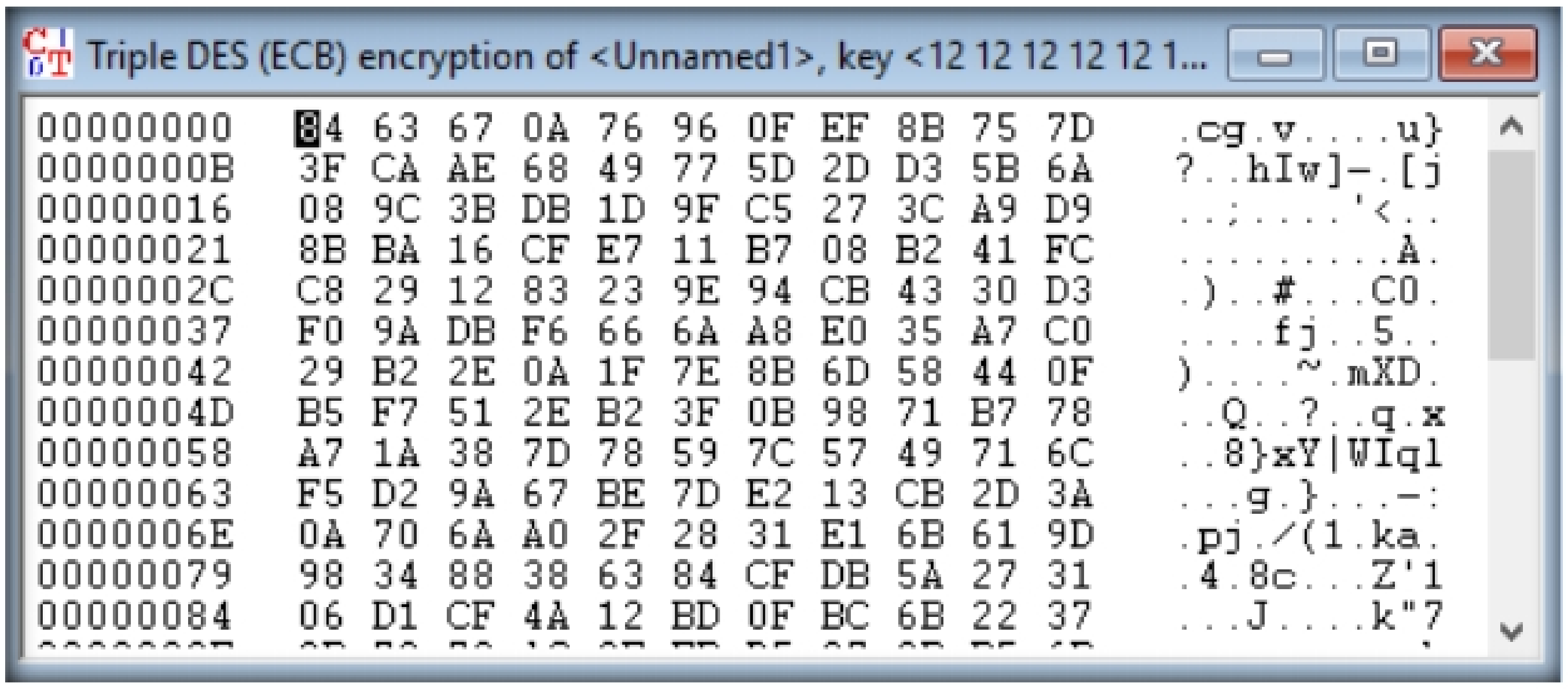
Enter the key using hexadecimal characters (0..9, A..F).

Key length: 128 bits (effectively 112 bits)

12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12

Figure 5.1.17: Key Entry: Triple DES (ECB) dialog-box

37. The **Triple DES (ECB) encryption of Unnamed1** notepad appears, as shown in the screenshot.


Triple DES (ECB) encryption of <Unnamed1>, key <12 12 12 12 12 1...

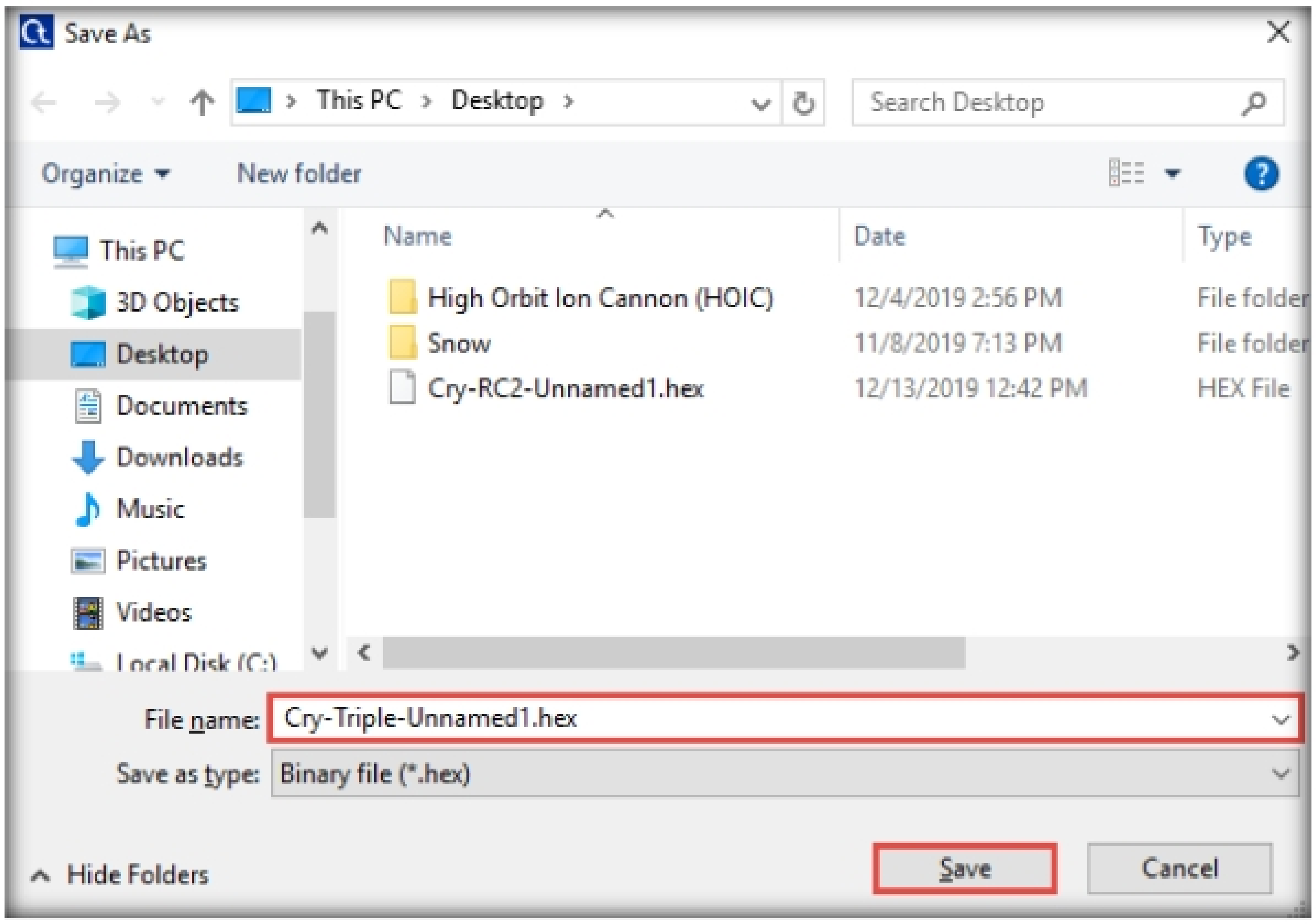
```
00000000   84 63 67 0A 76 96 0F EF 8B 75 7D    .cg.v....u}
0000000B   3F CA AE 68 49 77 5D 2D D3 5B 6A    ?..hIw]-.[j
00000016   08 9C 3B DB 1D 9F C5 27 3C A9 D9    ..;....'<..
00000021   8B BA 16 CF E7 11 B7 08 B2 41 FC    .........A.
0000002C   C8 29 12 83 23 9E 94 CB 43 30 D3    .)..#...C0.
00000037   F0 9A DB F6 66 6A A8 E0 35 A7 C0    ....fj..5..
00000042   29 B2 2E 0A 1F 7E 8B 6D 58 44 0F    )....~.mXD.
0000004D   B5 F7 51 2E B2 3F 0B 98 71 B7 78    ..Q..?..q.x
00000058   A7 1A 38 7D 78 59 7C 57 49 71 6C    ..8}xY|WIql
00000063   F5 D2 9A 67 BE 7D E2 13 CB 2D 3A    ...g.}...-:
0000006E   0A 70 6A A0 2F 28 31 E1 6B 61 9D    .pj./(1.ka.
00000079   98 34 88 38 63 84 CF DB 5A 27 31    .4.8c...Z'1
00000084   06 D1 CF 4A 12 BD 0F BC 6B 22 37    ...J....k"7
```

Figure 5.1.18: Output of RC2: encrypted data

38. To save the file, click **File** in the menu bar and select **Save**.

39. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

Note: The file name may differ in your lab environment.


Save As
This PC > Desktop >
Search Desktop
Organize ▾
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
Hide Folders
Save
Cancel

Name	Date	Type
High Orbit Ion Cannon (HOIC)	12/4/2019 2:56 PM	File folder
Snow	11/8/2019 7:13 PM	File folder
Cry-RC2-Unnamed1.hex	12/13/2019 12:42 PM	HEX File

File name: Cry-Triple-Unnamed1.hex

Save as type: Binary file (*.hex)

Figure 5.1.19: Save As window

40. To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.

TASK 1.5

Decrypt the Data

41. Switch to **Windows Server 2019**; copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.

42. Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**

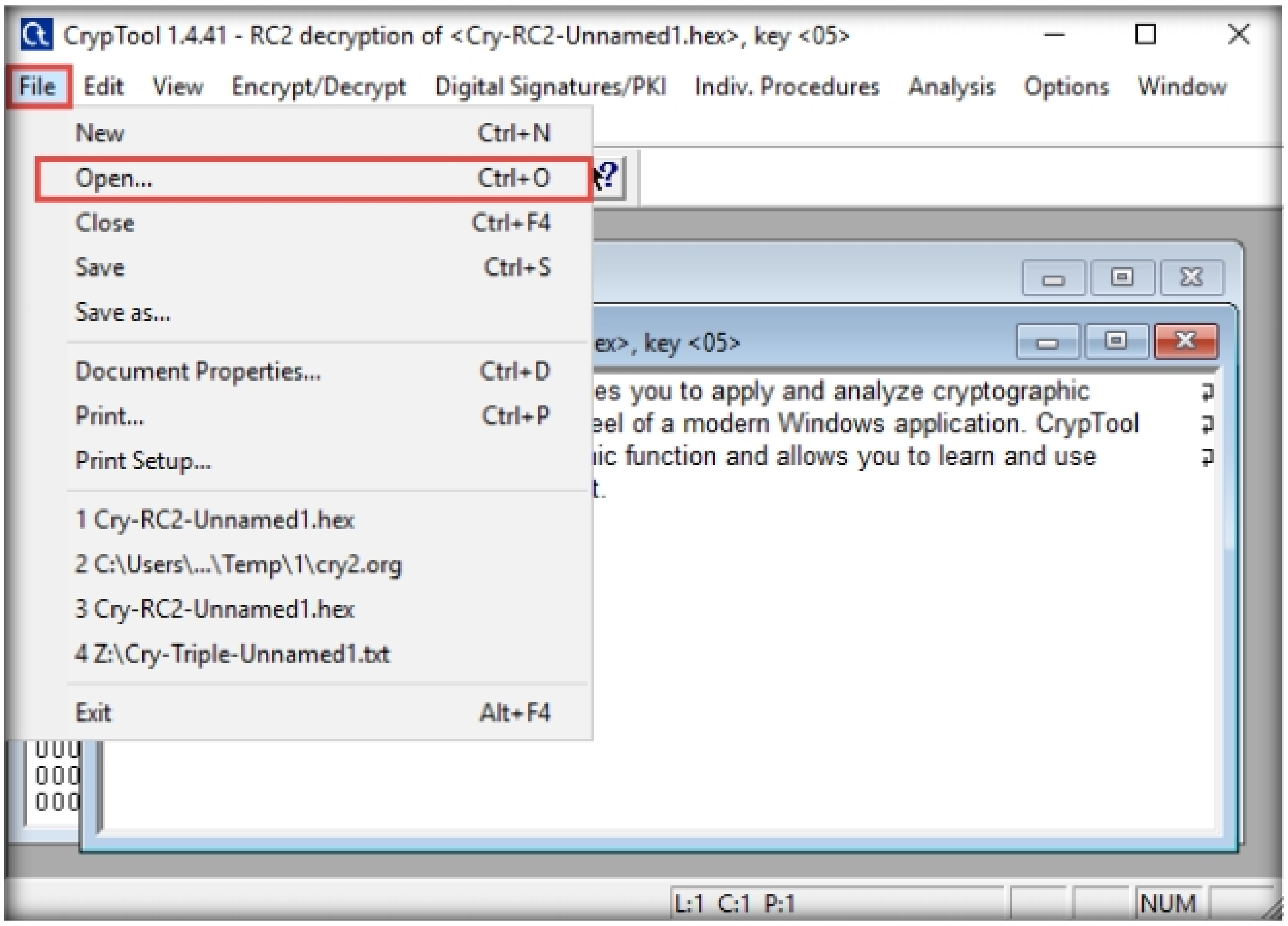
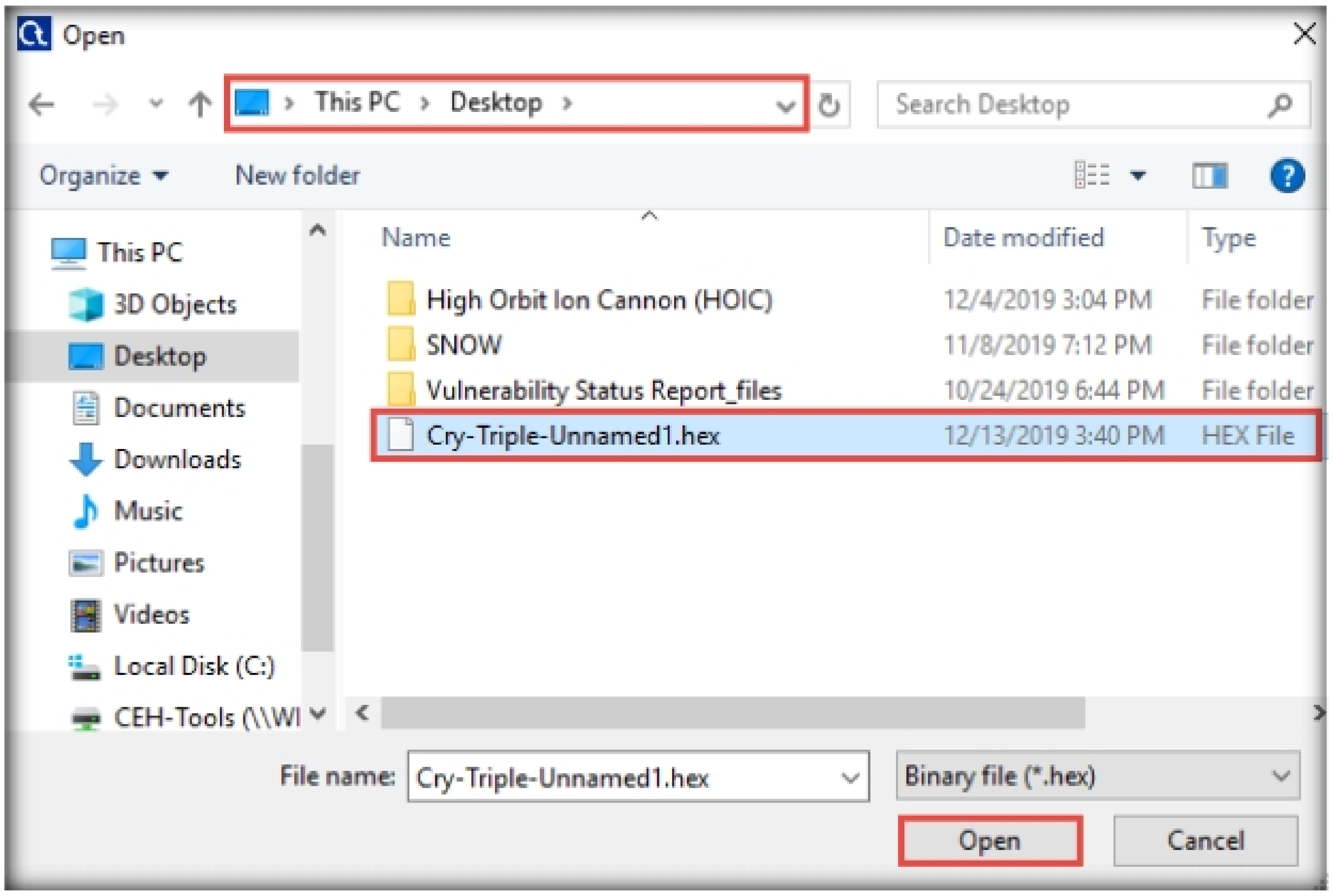

CrypTool 1.4.41 - RC2 decryption of <Cry-RC2-Unnamed1.hex>, key <05>
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
New Ctrl+N
Open... Ctrl+O
Close Ctrl+F4
Save Ctrl+S
Save as...
Document Properties... Ctrl+D
Print... Ctrl+P
Print Setup...
1 Cry-RC2-Unnamed1.hex
2 C:\Users\...\Temp\1\cry2.org
3 Cry-RC2-Unnamed1.hex
4 Z:\Cry-Triple-Unnamed1.txt
Exit Alt+F4
L:1 C:1 P:1
NUM

Figure 5.1.20: Opening a Crypted file

43. The **Open** window appears; select **Binary file (*.hex)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.


Open
This PC > Desktop >
Search Desktop
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CEH-Tools (\\WI
Open
Cancel

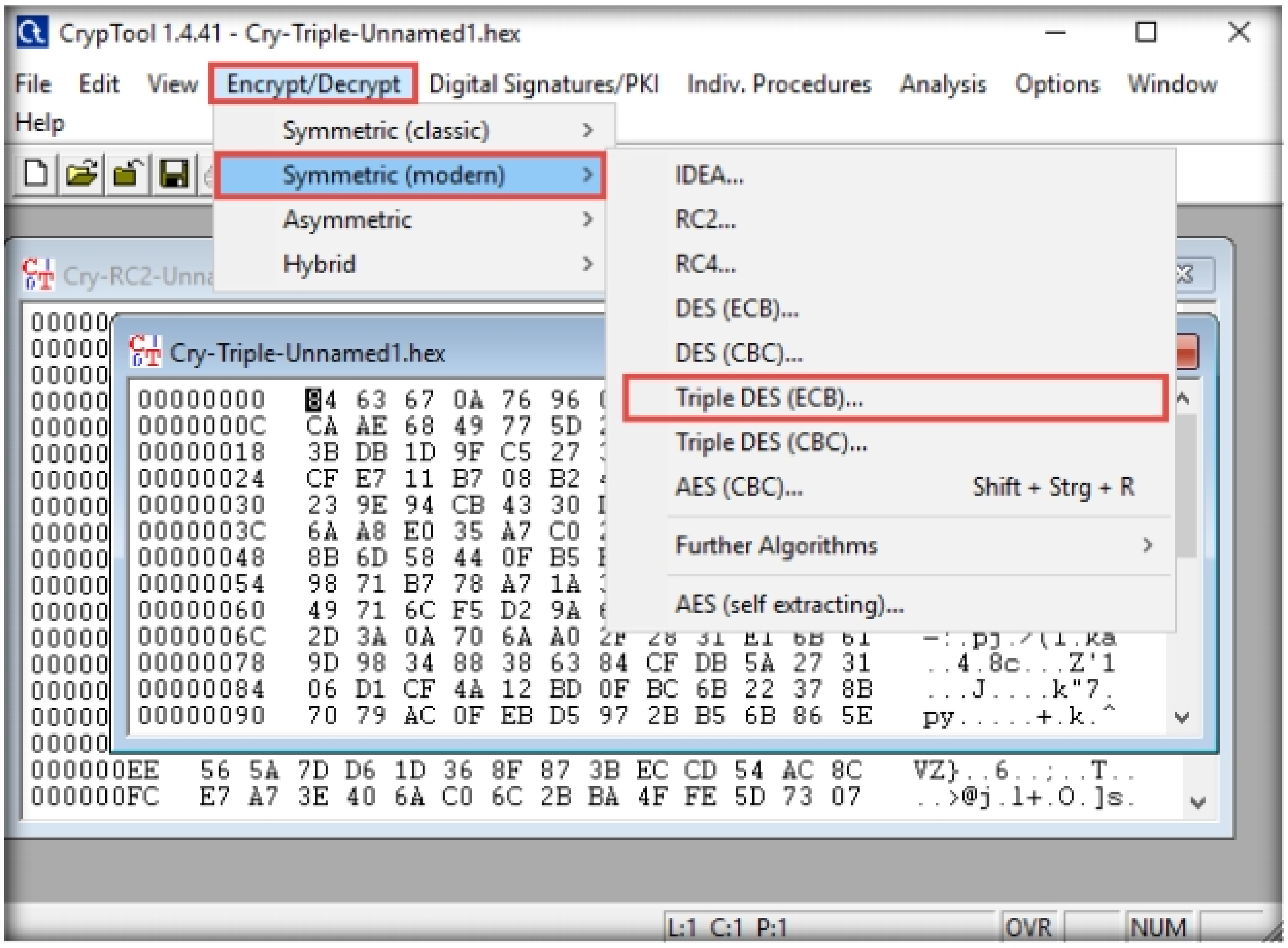
Name	Date modified	Type
High Orbit Ion Cannon (HOIC)	12/4/2019 3:04 PM	File folder
SNOW	11/8/2019 7:12 PM	File folder
Vulnerability Status Report_files	10/24/2019 6:44 PM	File folder
Cry-Triple-Unnamed1.hex	12/13/2019 3:40 PM	HEX File

File name: Cry-Triple-Unnamed1.hex

Binary file (*.hex)

Figure 5.1.21: Opening a Crypted file

44. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) → Triple DES (ECB)...**

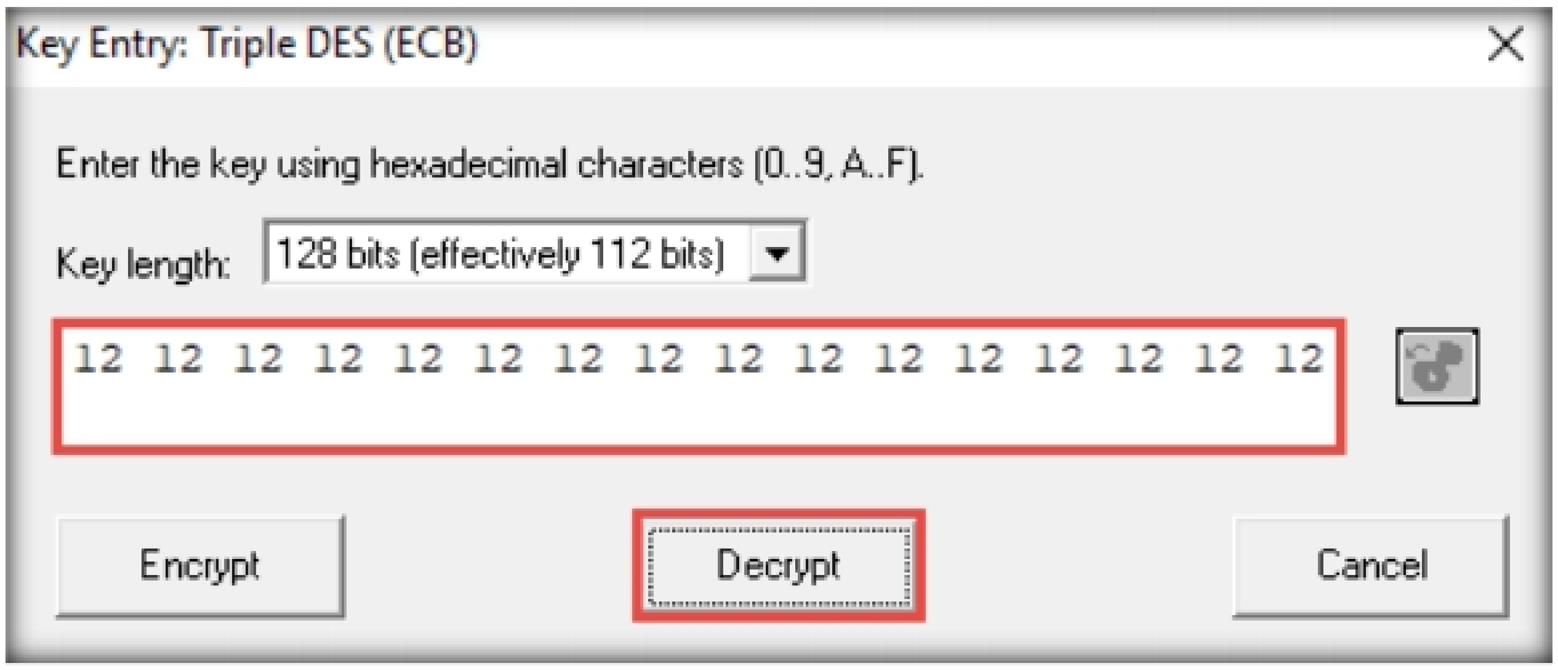

CrypTool 1.4.41 - Cry-Triple-Unnamed1.hex
File
Edit
View
Encrypt/Decrypt
Digital Signatures/PKI
Indiv. Procedures
Analysis
Options
Window
Help
Symmetric (classic)
Symmetric (modern)
Asymmetric
Hybrid
IDEA...
RC2...
RC4...
DES (ECB)...
DES (CBC)...
Triple DES (ECB)...
Triple DES (CBC)...
AES (CBC)...
Shift + Strg + R
Further Algorithms
AES (self extracting)...
Cry-RC2-Unna
Cry-Triple-Unnamed1.hex
L:1 C:1 P:1
OVR
NUM

```
00000000  84 63 67 0A 76 96
0000000C  CA AE 68 49 77 5D
00000018  3B DB 1D 9F C5 27
00000024  CF E7 11 B7 08 B2
00000030  23 9E 94 CB 43 30
0000003C  6A A8 E0 35 A7 C0
00000048  8B 6D 58 44 0F B5
00000054  98 71 B7 78 A7 1A
00000060  49 71 6C F5 D2 9A
0000006C  2D 3A 0A 70 6A A0 2F 28 31 E1 6B 61   -:.pj./(1.ka
00000078  9D 98 34 88 38 63 84 CF DB 5A 27 31   ..4.8c...Z'1
00000084  06 D1 CF 4A 12 BD 0F BC 6B 22 37 8B   ...J....k"7.
00000090  70 79 AC 0F EB D5 97 2B B5 6B 86 5E   py.....+.k.^

000000EE   56 5A 7D D6 1D 36 8F 87 3B EC CD 54 AC 8C   VZ}..6..;..T..
000000FC   E7 A7 3E 40 6A C0 6C 2B BA 4F FE 5D 73 07   ..>@j.l+.O.]s.
```

Figure 5.1.22: Select the Triple DES Encryption algorithm

45. The **Key Entry: Triple DES (ECB)** dialog-box appears; keep the **Key length** set to default (**128 bits (effectively 112 bits)**).

46. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.


Key Entry: Triple DES (ECB)
Encrypt
Decrypt
Cancel

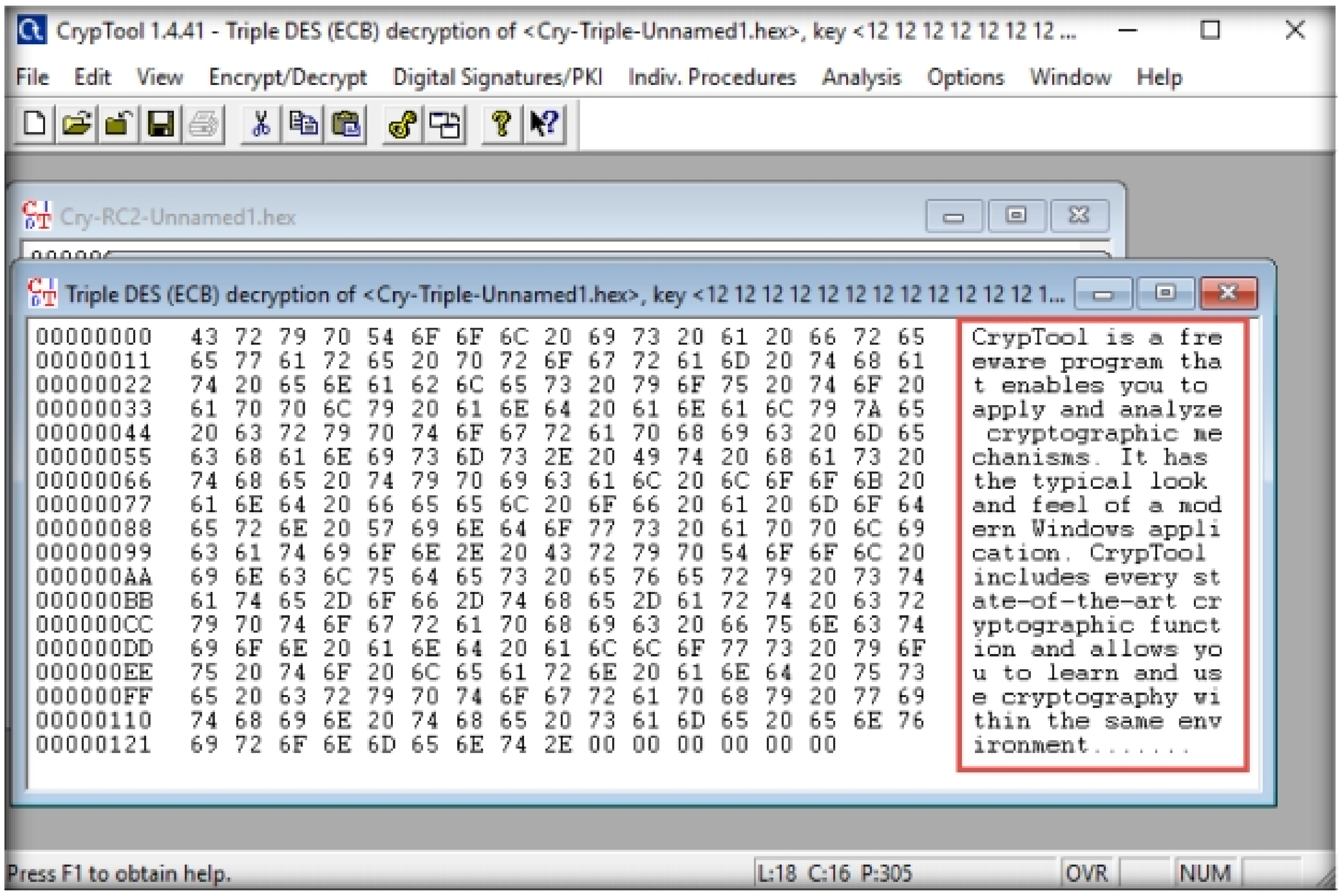
Enter the key using hexadecimal characters (0..9, A..F).

Key length: 128 bits (effectively 112 bits)

12 12 12 12 12 12 12 12 12 12 12 12 12 12 12 12

Figure 5.1.23: Key Entry: Triple DES (ECB) dialog-box

47. The decrypted text appears, as shown in the screenshot.


CrypTool 1.4.41 - Triple DES (ECB) decryption of <Cry-Triple-Unnamed1.hex>, key <12 12 12 12 12 12 12 ...
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Cry-RC2-Unnamed1.hex
Triple DES (ECB) decryption of <Cry-Triple-Unnamed1.hex>, key <12 12 12 12 12 12 12 12 12 12 12 12 1...
Press F1 to obtain help.
L:18 C:16 P:305
OVR
NUM

```
00000000   43 72 79 70 54 6F 6F 6C 20 69 73 20 61 20 66 72 65   CrypTool is a fre
00000011   65 77 61 72 65 20 70 72 6F 67 72 61 6D 20 74 68 61   eware program tha
00000022   74 20 65 6E 61 62 6C 65 73 20 79 6F 75 20 74 6F 20   t enables you to
00000033   61 70 70 6C 79 20 61 6E 64 20 61 6E 61 6C 79 7A 65   apply and analyze
00000044   20 63 72 79 70 74 6F 67 72 61 70 68 69 63 20 6D 65    cryptographic me
00000055   63 68 61 6E 69 73 6D 73 2E 20 49 74 20 68 61 73 20   chanisms. It has
00000066   74 68 65 20 74 79 70 69 63 61 6C 20 6C 6F 6F 6B 20   the typical look
00000077   61 6E 64 20 66 65 65 6C 20 6F 66 20 61 20 6D 6F 64   and feel of a mod
00000088   65 72 6E 20 57 69 6E 64 6F 77 73 20 61 70 70 6C 69   ern Windows appli
00000099   63 61 74 69 6F 6E 2E 20 43 72 79 70 54 6F 6F 6C 20   cation. CrypTool
000000AA   69 6E 63 6C 75 64 65 73 20 65 76 65 72 79 20 73 74   includes every st
000000BB   61 74 65 2D 6F 66 2D 74 68 65 2D 61 72 74 20 63 72   ate-of-the-art cr
000000CC   79 70 74 6F 67 72 61 70 68 69 63 20 66 75 6E 63 74   yptographic funct
000000DD   69 6F 6E 20 61 6E 64 20 61 6C 6C 6F 77 73 20 79 6F   ion and allows yo
000000EE   75 20 74 6F 20 6C 65 61 72 6E 20 61 6E 64 20 75 73   u to learn and us
000000FF   65 20 63 72 79 70 74 6F 67 72 61 70 68 79 20 77 69   e cryptography wi
00000110   74 68 69 6E 20 74 68 65 20 73 61 6D 65 20 65 6E 76   thin the same env
00000121   69 72 6F 6E 6D 65 6E 74 2E 00 00 00 00 00 00         ironment.......
```

Figure 5.1.24: Decrypted the file successfully

48. Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.

49. This concludes the demonstration of performing cryptanalysis using CrypTool.

50. Close all open windows and document all the acquired information.

TASK 2

Perform Cryptanalysis using AlphaPeeler

Here, we will use the AlphaPeeler tool to perform cryptanalysis.

TASK 2.1

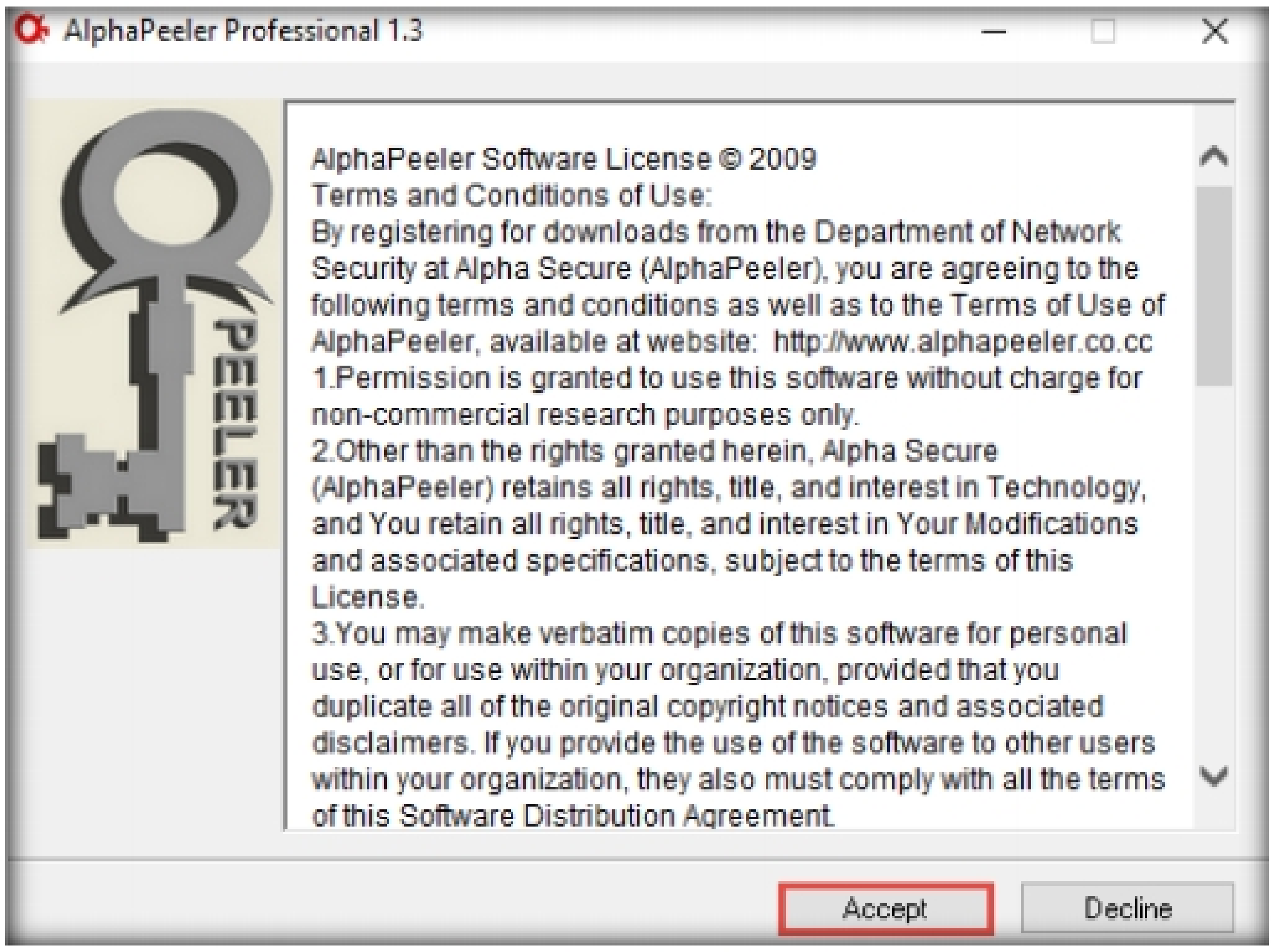
Install and Launch AlphaPeeler

1. In the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and double-click **AlphaPeelerPro1.3wse.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor's teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher.

2. The **AlphaPeeler Professional** window appears; click **Accept**.



AlphaPeeler Professional 1.3
PEELER
Accept
Decline

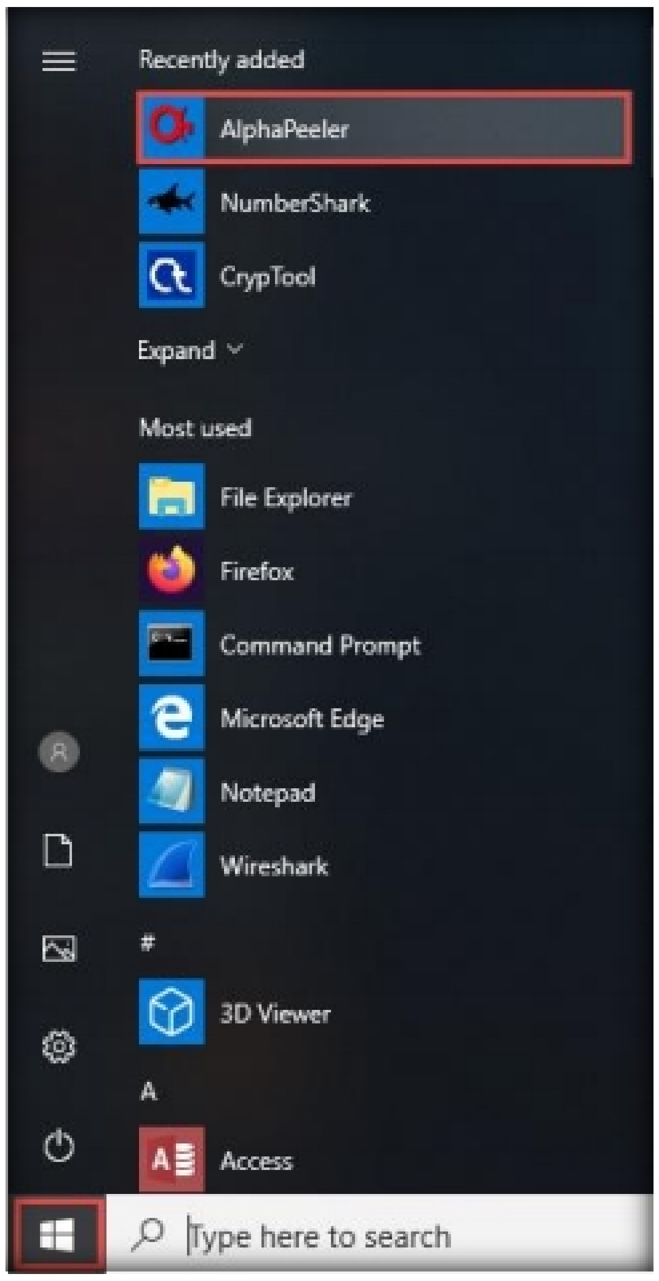
AlphaPeeler Software License © 2009
Terms and Conditions of Use:
By registering for downloads from the Department of Network Security at Alpha Secure (AlphaPeeler), you are agreeing to the following terms and conditions as well as to the Terms of Use of AlphaPeeler, available at website: http://www.alphapeeler.co.cc
1.Permission is granted to use this software without charge for non-commercial research purposes only.
2.Other than the rights granted herein, Alpha Secure (AlphaPeeler) retains all rights, title, and interest in Technology, and You retain all rights, title, and interest in Your Modifications and associated specifications, subject to the terms of this License.
3.You may make verbatim copies of this software for personal use, or for use within your organization, provided that you duplicate all of the original copyright notices and associated disclaimers. If you provide the use of the software to other users within your organization, they also must comply with all the terms of this Software Distribution Agreement.

Figure 5.2.1: AlphaPeeler Professional setup

3. Follow the steps in the wizard and install the application using all default settings.

AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

4. After the completion of the installation, click the **Start** icon from the bottom-left corner of **Desktop** and click **AlphaPeeler** from the applications.



Recently added
AlphaPeeler
NumberShark
CrypTool
Expand
Most used
File Explorer
Firefox
Command Prompt
Microsoft Edge
Notepad
Wireshark
#
3D Viewer
A
Access
Type here to search

Figure 5.2.2: Launch AlphaPeeler

5. **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.

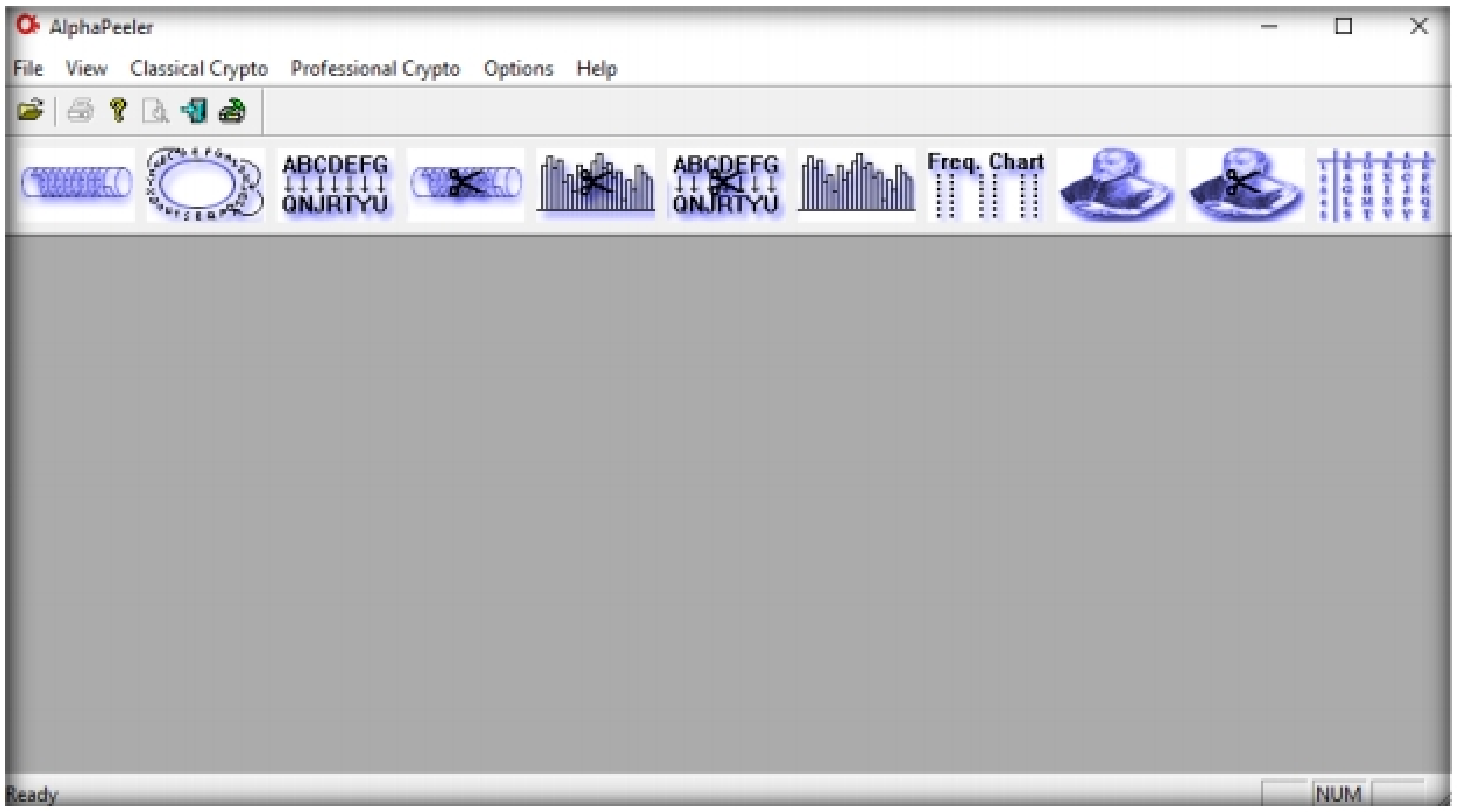
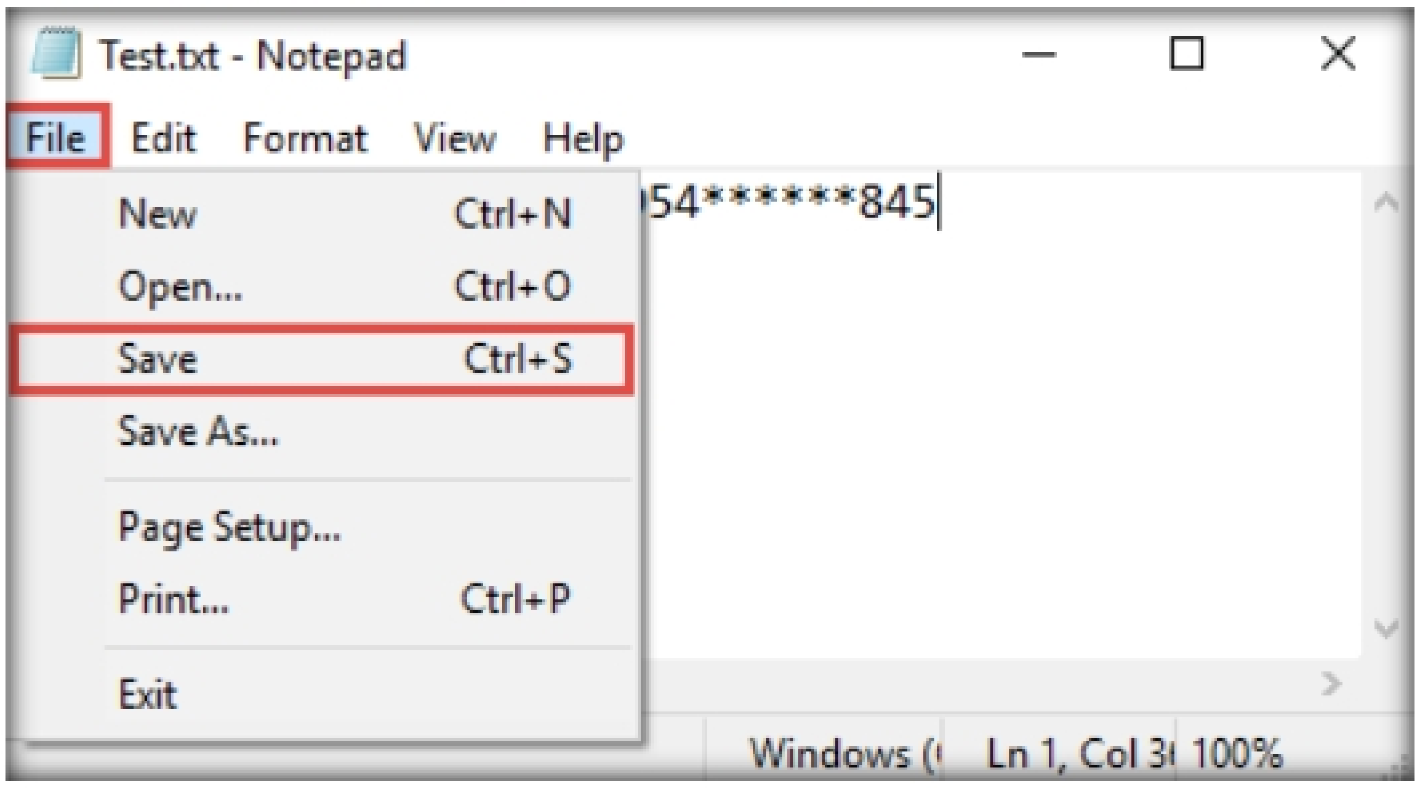

AlphaPeeler
File View Classical Crypto Professional Crypto Options Help
ABCDEFG QNJRTYU
Freq. Chart
Ready
NUM

Figure 5.2.3: AlphaPeeler window

6. Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.

7. Click **File** in the menu bar and click **Save**.


Test.txt - Notepad
File Edit Format View Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Page Setup...
Print... Ctrl+P
Exit
Windows (
Ln 1, Col 3
100%

54******845

Figure 5.2.4: Text file

TASK 2.2

Encrypt a Data File

8. Switch back to the **AlphaPeeler** window; click **Professional Crypto** from the menu bar and select **DES crypto** from the options.

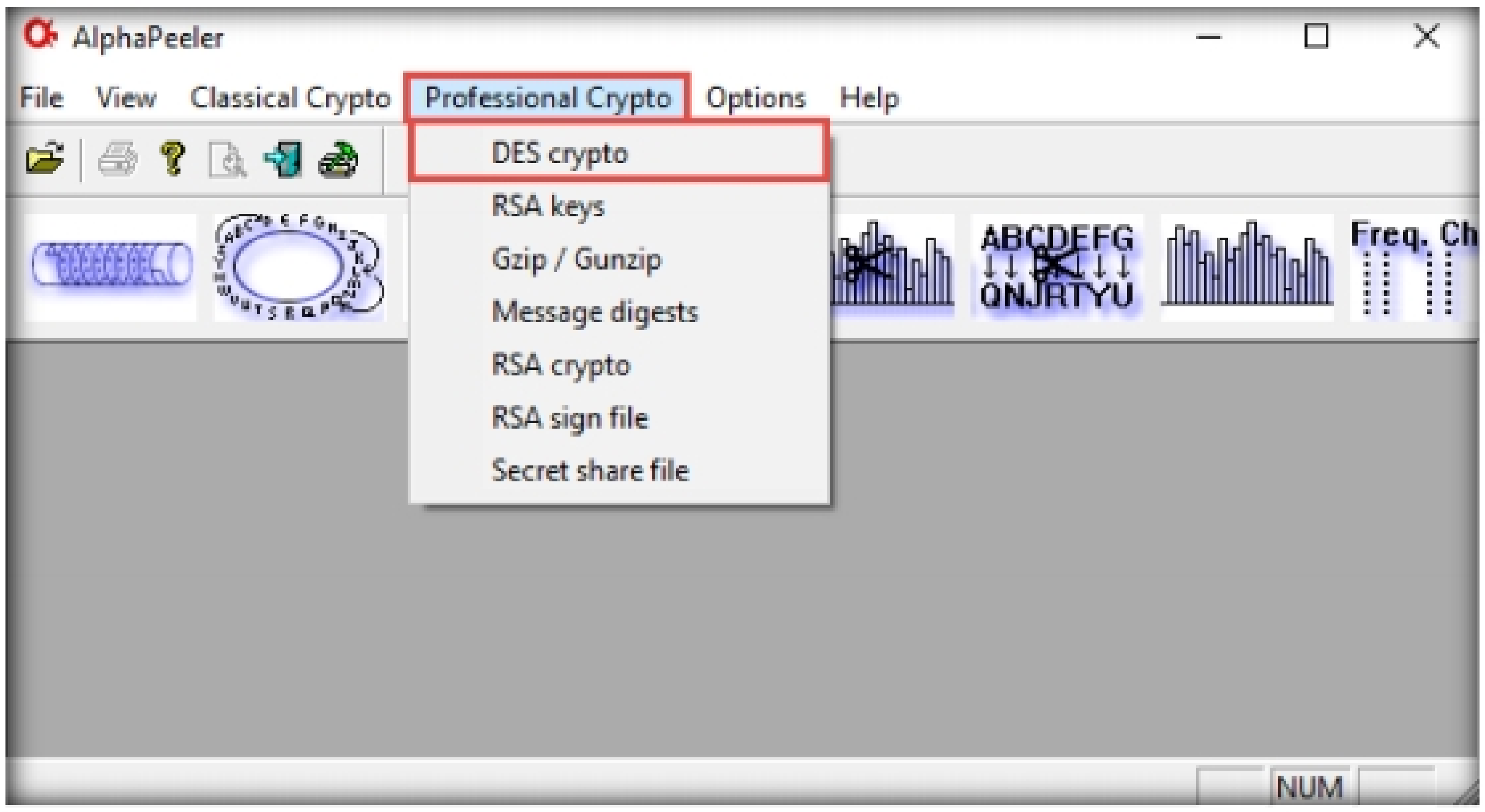

AlphaPeeler
File
View
Classical Crypto
Professional Crypto
Options
Help
DES crypto
RSA keys
Gzip / Gunzip
Message digests
RSA crypto
RSA sign file
Secret share file
ABCDEFG
QNJRTYU
Freq. Ch
NUM

Figure 5.2.5: Selecting DES crypto

9. The **DES crypto** pop-up appears; click the ellipsis icon (..) under the **Plain text file** option.

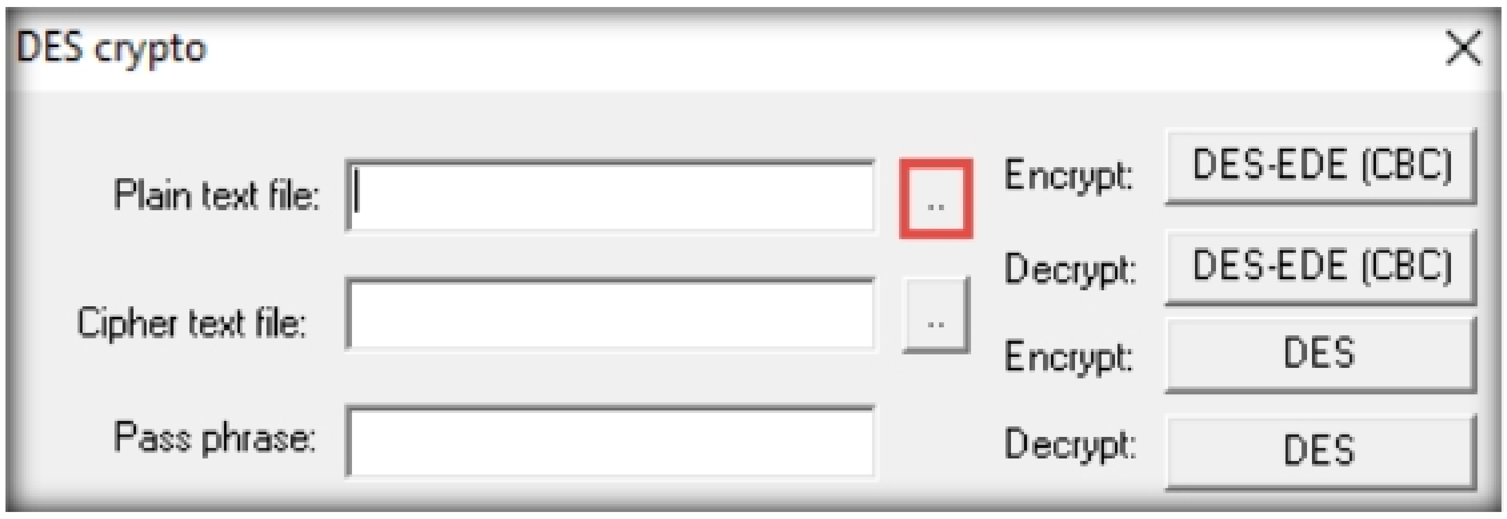

DES crypto
Plain text file:
..
Cipher text file:
..
Pass phrase:
Encrypt:
DES-EDE (CBC)
Decrypt:
DES-EDE (CBC)
Encrypt:
DES
Decrypt:
DES

Figure 5.2.6: Selecting DES crypto

10. The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

Note: Here, we are selecting the file that we will encrypt and this will act as an input file.

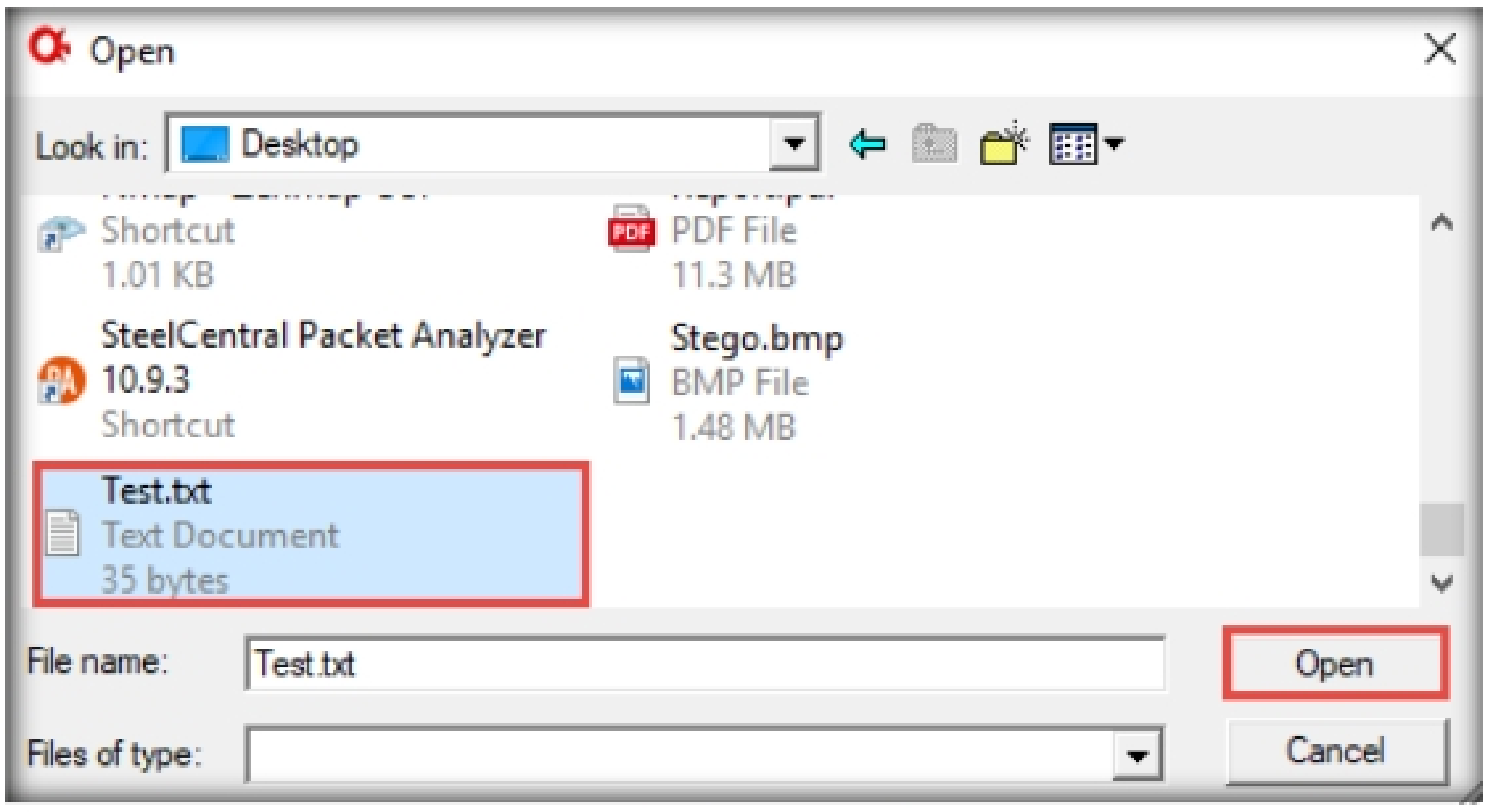

Open
Look in:
Desktop
Shortcut
1.01 KB
PDF File
11.3 MB
SteelCentral Packet Analyzer 10.9.3
Shortcut
Stego.bmp
BMP File
1.48 MB
Test.txt
Text Document
35 bytes
File name:
Test.txt
Files of type:
Open
Cancel

Figure 5.2.7: Open window

11. In the **DES crypto** pop-up; click the ellipsis icon (..) under the **Cipher text file** option.

12. The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.

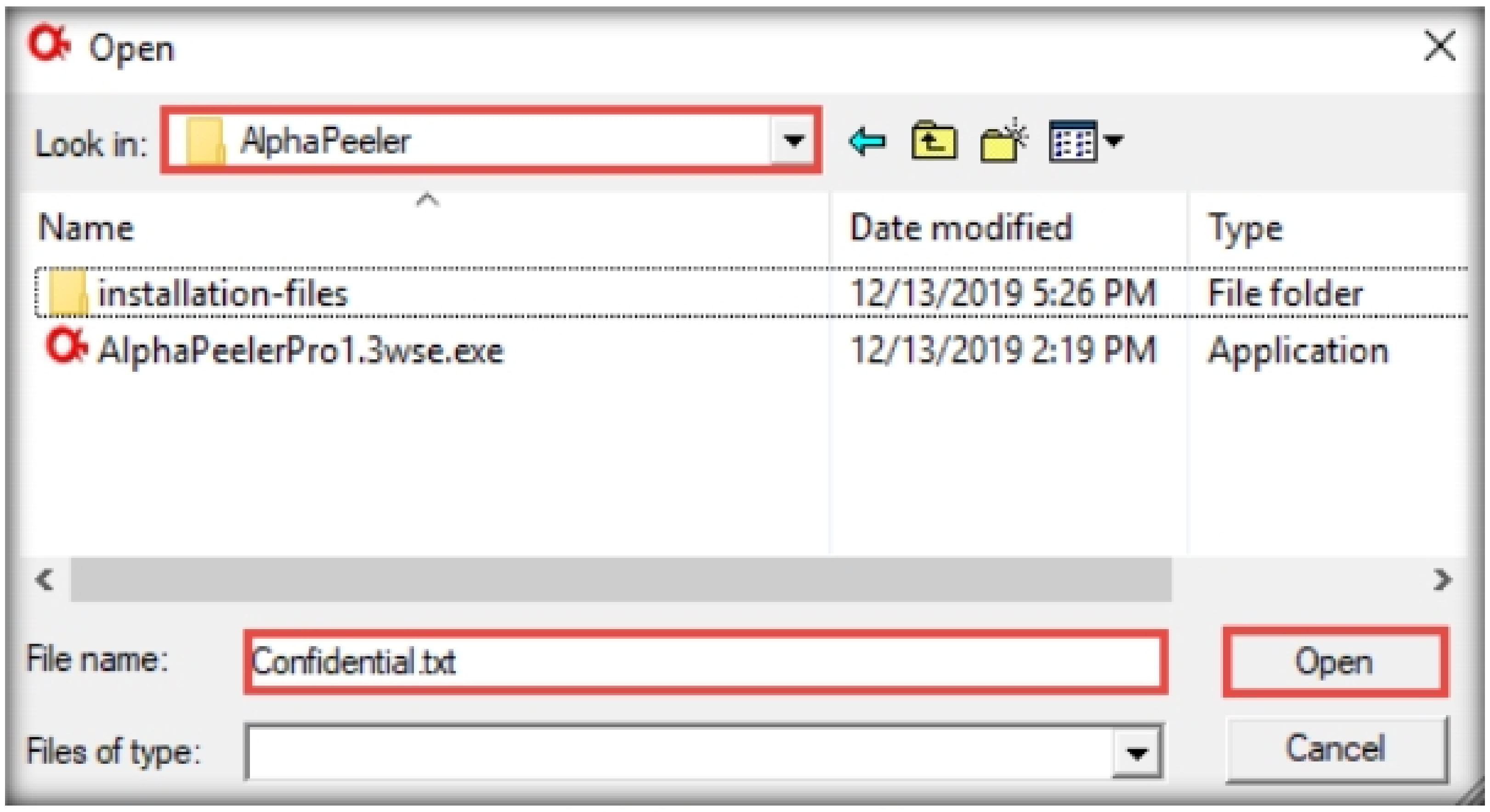

Open
Look in:
AlphaPeeler
Name
Date modified
Type
installation-files
12/13/2019 5:26 PM
File folder
AlphaPeelerPro1.3wse.exe
12/13/2019 2:19 PM
Application
File name:
Confidential.txt
Open
Files of type:
Cancel

Figure 5.2.8: Open window

13. In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** to encrypt the text file.

Note: Here, the password provided is **test@123**.

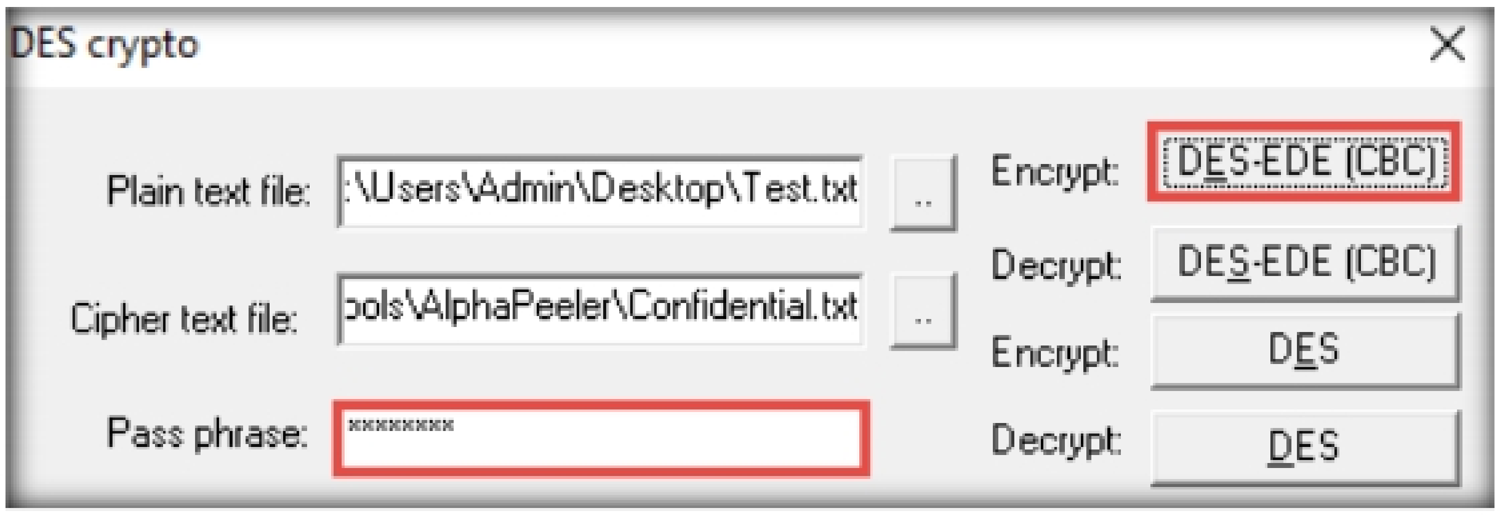
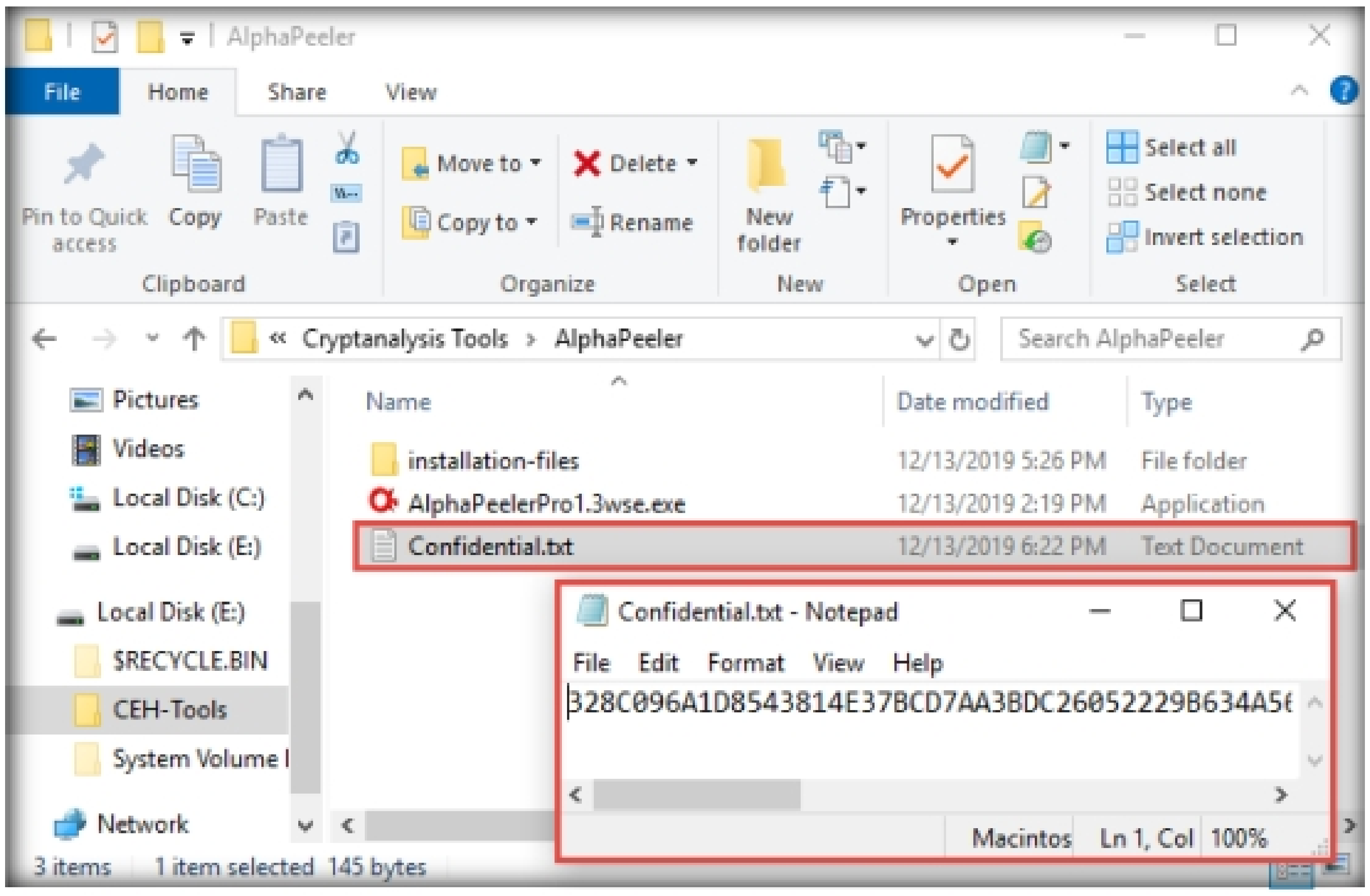

DES crypto
Plain text file:
:\Users\Admin\Desktop\Test.txt
Cipher text file:
pols\AlphaPeeler\Confidential.txt
Pass phrase:
****
Encrypt:
DES-EDE (CBC)
Decrypt:
DES-EDE (CBC)
Encrypt:
DES
Decrypt:
DES

Figure 5.2.9: DES crypto

14. A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.

15. Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

Note: Here, the encrypted file is shared through shared network drive **E\CEH-Tools\ CEHv11 Module 20 Cryptography** and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and view the data in plain-text.


AlphaPeeler
File
Home
Share
View
Pin to Quick access
Copy
Paste
Move to
Copy to
Delete
Rename
New folder
Properties
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
« Cryptanalysis Tools › AlphaPeeler
Search AlphaPeeler
Pictures
Videos
Local Disk (C:)
Local Disk (E:)
Local Disk (E:)
$RECYCLE.BIN
CEH-Tools
System Volume I
Network
Name
Date modified
Type
installation-files
12/13/2019 5:26 PM
File folder
AlphaPeelerPro1.3wse.exe
12/13/2019 2:19 PM
Application
Confidential.txt
12/13/2019 6:22 PM
Text Document
Confidential.txt - Notepad
File Edit Format View Help
Macintos
Ln 1, Col
100%
3 items
1 item selected 145 bytes

328C096A1D8543814E37BCD7AA3BDC26052229B634A5

Figure 5.2.10: Confidential.txt file

16. Close the **DES crypto** pop-up and the **AlphaPeeler** window.

17. Switch to **Windows Server 2019**; navigate to **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and copy the **AlphaPeelerPro1.3wse.exe** file on **Desktop**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

18. Follow the steps in the wizard and install the application using all default settings.

19. After completion of the installation; click the **Start** icon from the bottom-right corner of **Desktop** and click **AlphaPeeler** from the applications.

TASK 2.3

Decrypt a Data File

20. The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**

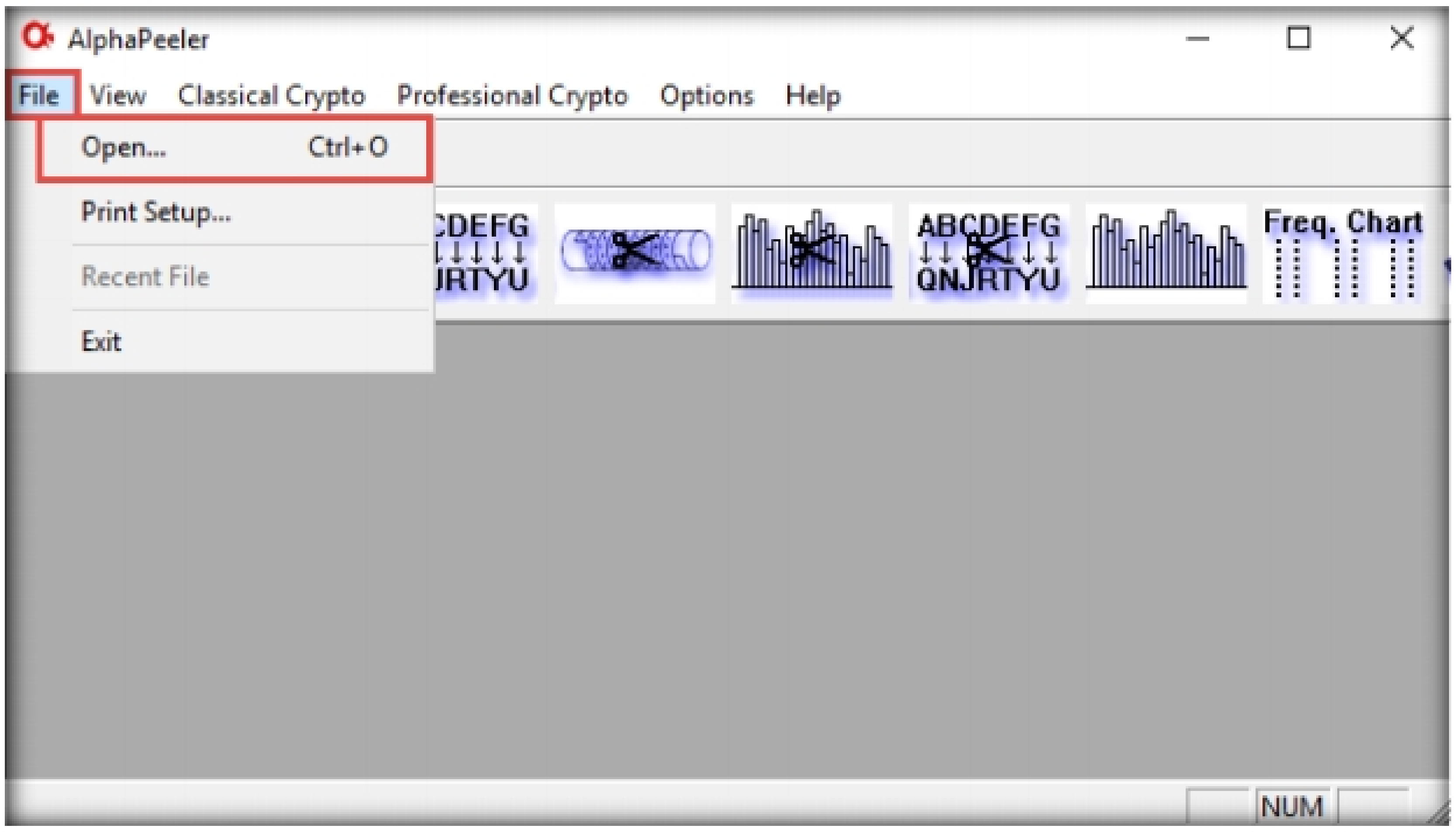
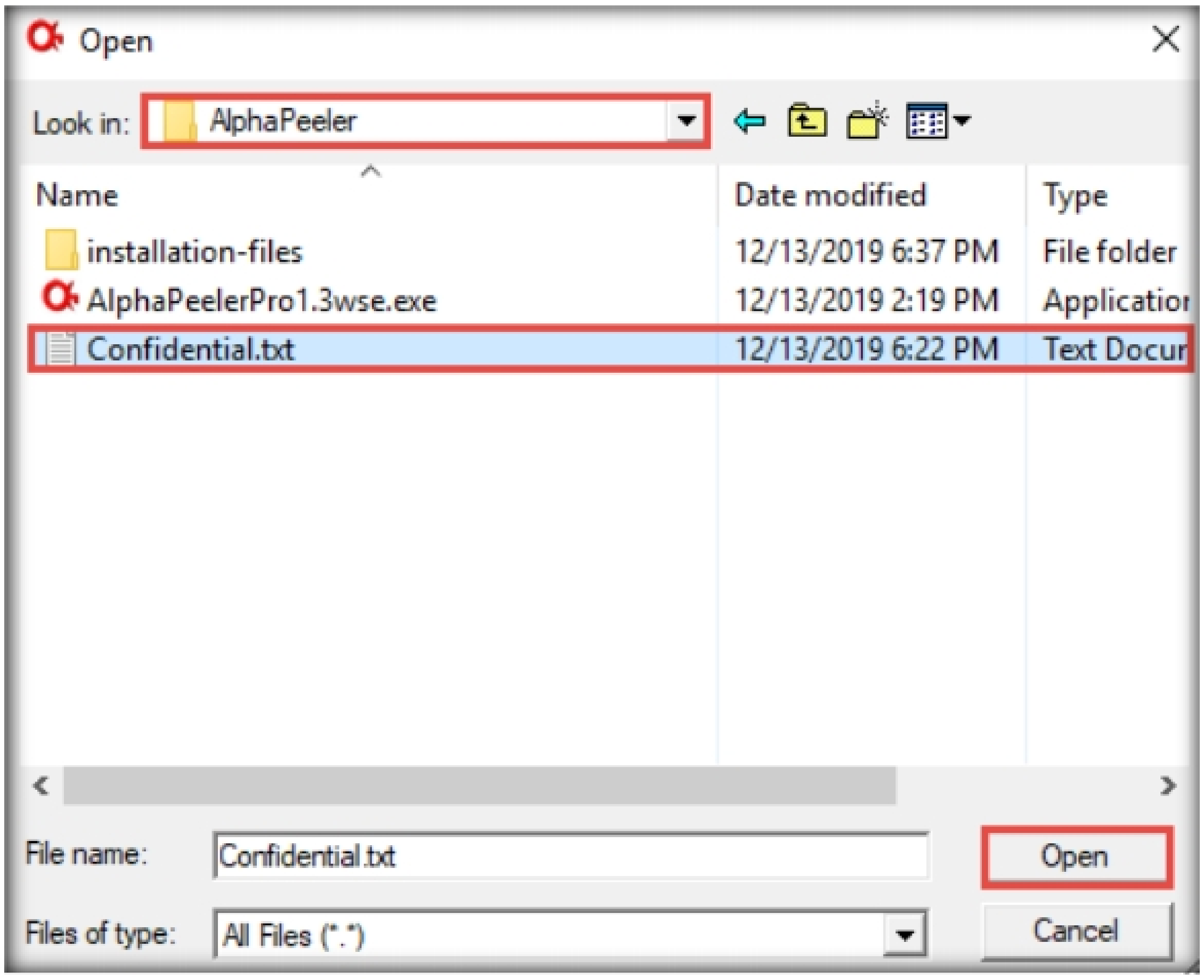

AlphaPeeler
File
View
Classical Crypto
Professional Crypto
Options
Help
Open... Ctrl+O
Print Setup...
Recent File
Exit
Freq. Chart
NUM

Figure 5.2.11: Confidential.txt file

21. The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.


Open
Look in:
AlphaPeeler
Open
Cancel

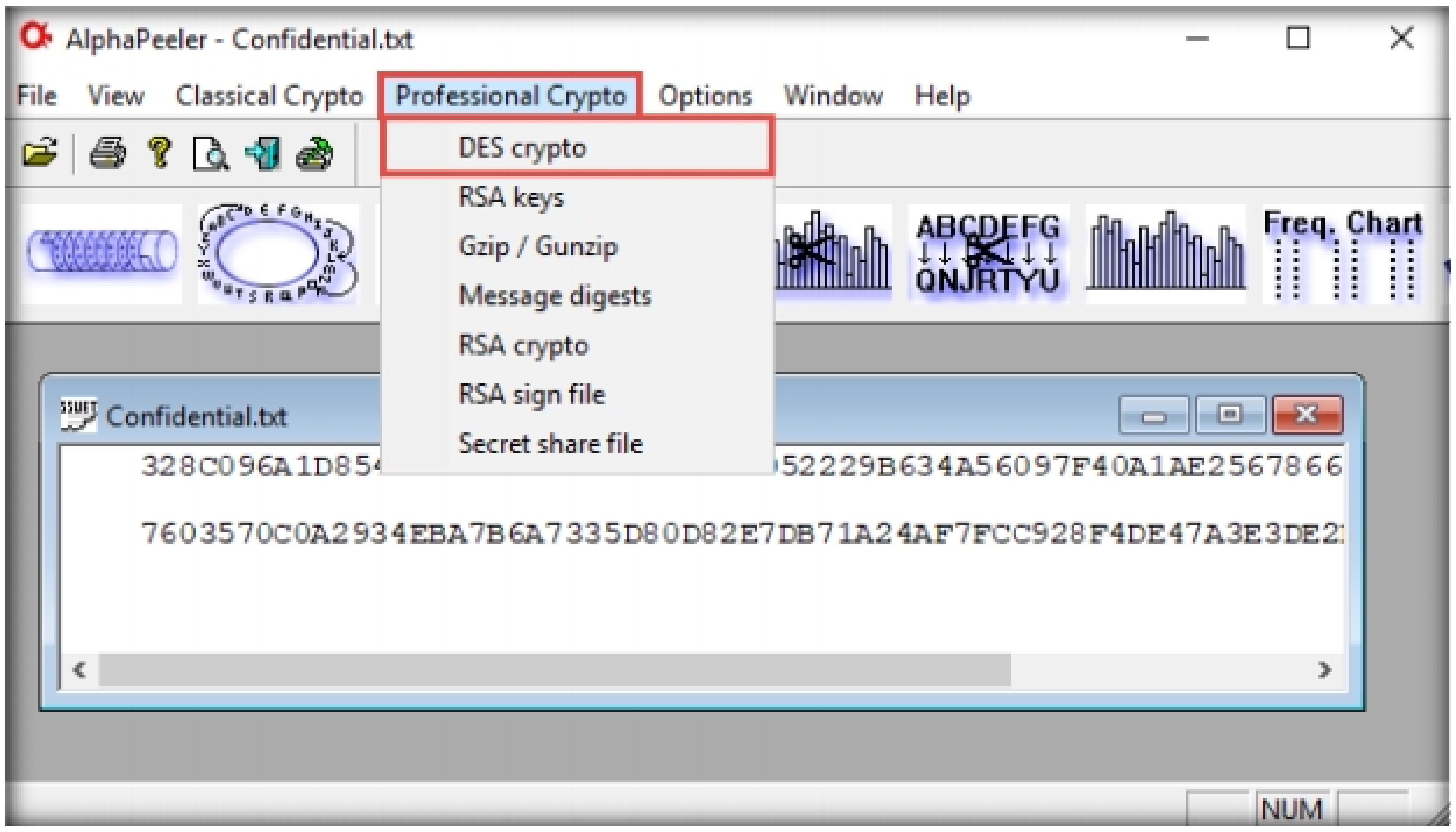
Name	Date modified	Type
installation-files	12/13/2019 6:37 PM	File folder
AlphaPeelerPro1.3wse.exe	12/13/2019 2:19 PM	Applicatior
Confidential.txt	12/13/2019 6:22 PM	Text Docur

File name: Confidential.txt

Files of type: All Files (*.*)

Figure 5.2.12: Open window select Confidential.txt file

22. The **Confidential.txt** file appears; click **Professional crypto** from the menu bar and select the **DES crypto** option.


AlphaPeeler - Confidential.txt
File
View
Classical Crypto
Professional Crypto
Options
Window
Help
DES crypto
RSA keys
Gzip / Gunzip
Message digests
RSA crypto
RSA sign file
Secret share file
ABCDEFG
QNJRTYU
Freq. Chart
Confidential.txt
NUM

```
328C096A1D85                    52229B634A56097F40A1AE2567866

7603570C0A2934EBA7B6A7335D80D82E7DB71A24AF7FCC928F4DE47A3E3DE2
```

Figure 5.2.13: Selecting DES crypto

23. The **DES crypto** pop-up appears; click the ellipsis icon (..) next to the **Plain text file** option.

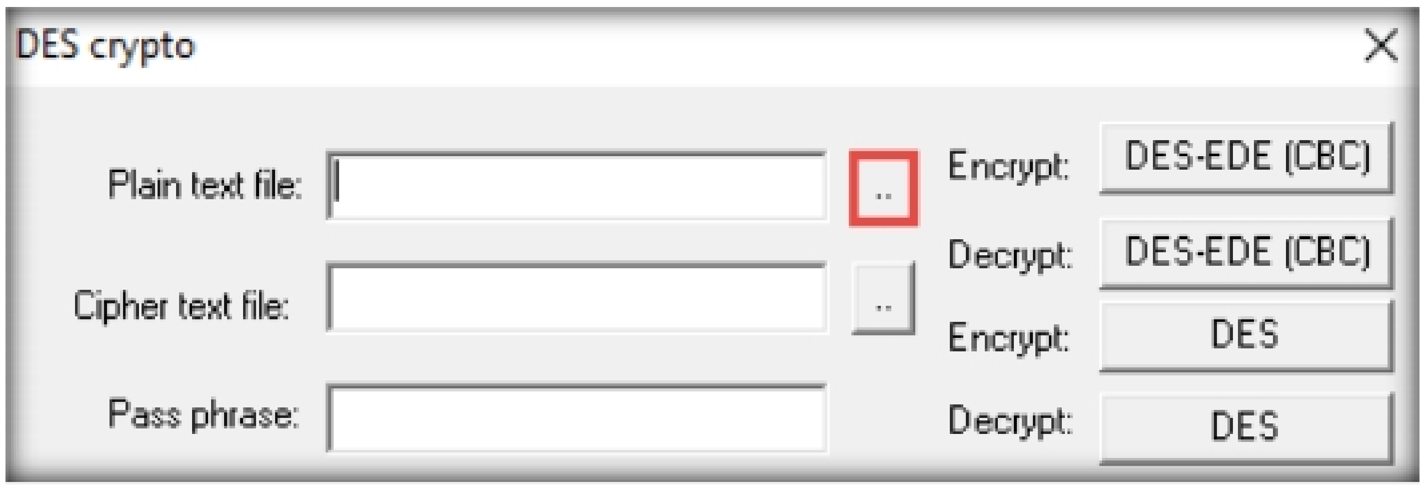

DES crypto
Plain text file:
..
Cipher text file:
..
Pass phrase:
Encrypt:
DES-EDE (CBC)
Decrypt:
DES-EDE (CBC)
Encrypt:
DES
Decrypt:
DES

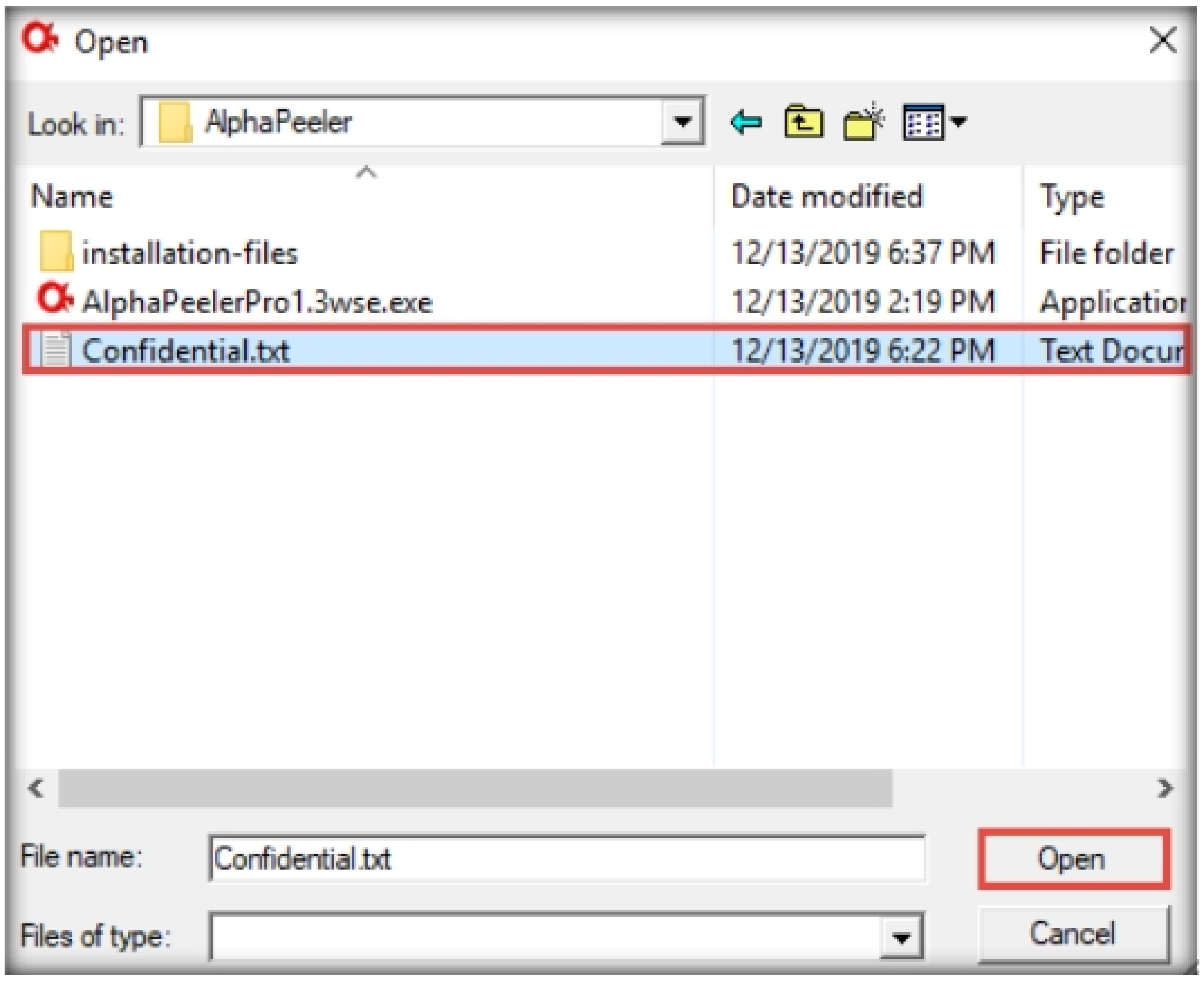
Figure 5.2.14: Selecting DES crypto

24. The **Open** window appears; navigate to **Desktop** and name the file **Result.txt**; then, click **Open**.

Note: Here, we are creating an output file that will be in plain-text.

25. In the **DES crypto** pop-up; click the ellipsis icon (..) under the **Cipher text file** option.

26. The **Open** window appears; select the encrypted file (**Confidential.txt**) located at **Z:\CEHv11 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and click **Open**.


Open
Open
Cancel
Files of type:

Look in: AlphaPeeler

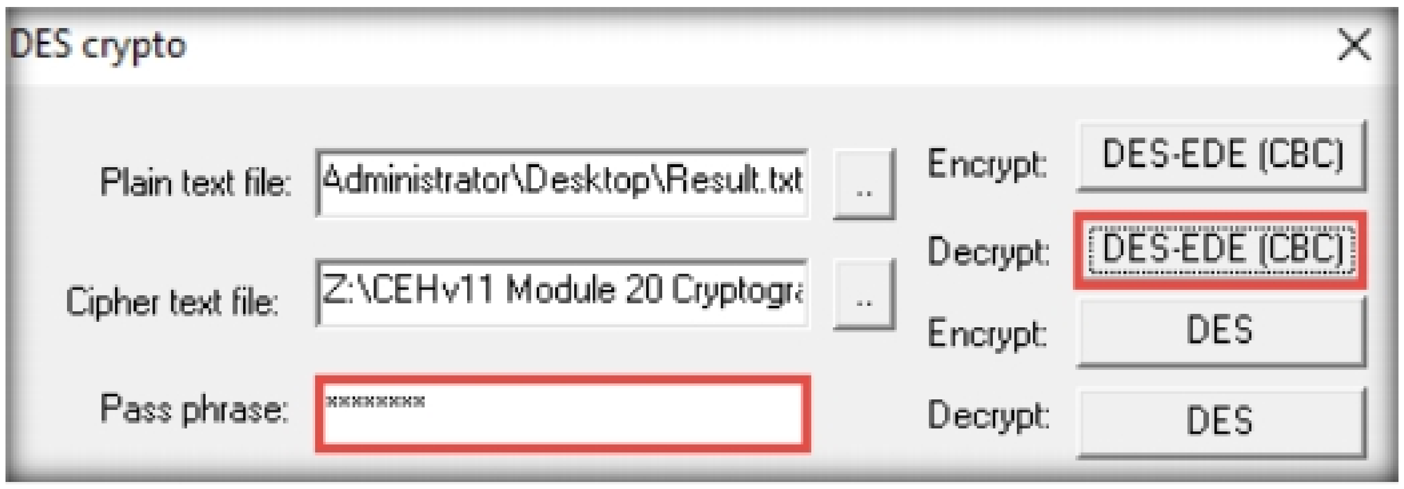
Name	Date modified	Type
installation-files	12/13/2019 6:37 PM	File folder
AlphaPeelerPro1.3wse.exe	12/13/2019 2:19 PM	Applicatior
Confidential.txt	12/13/2019 6:22 PM	Text Docur

File name: Confidential.txt

Figure 5.2.15: Open window

27. In the **DES crypto** pop-up, enter the password that you provided in **Step#13** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

Note: Here, the password provided is **test@123**.


DES crypto
Encrypt: DES-EDE (CBC)
Decrypt: DES-EDE (CBC)
Encrypt: DES
Decrypt: DES

Plain text file: Administrator\Desktop\Result.txt

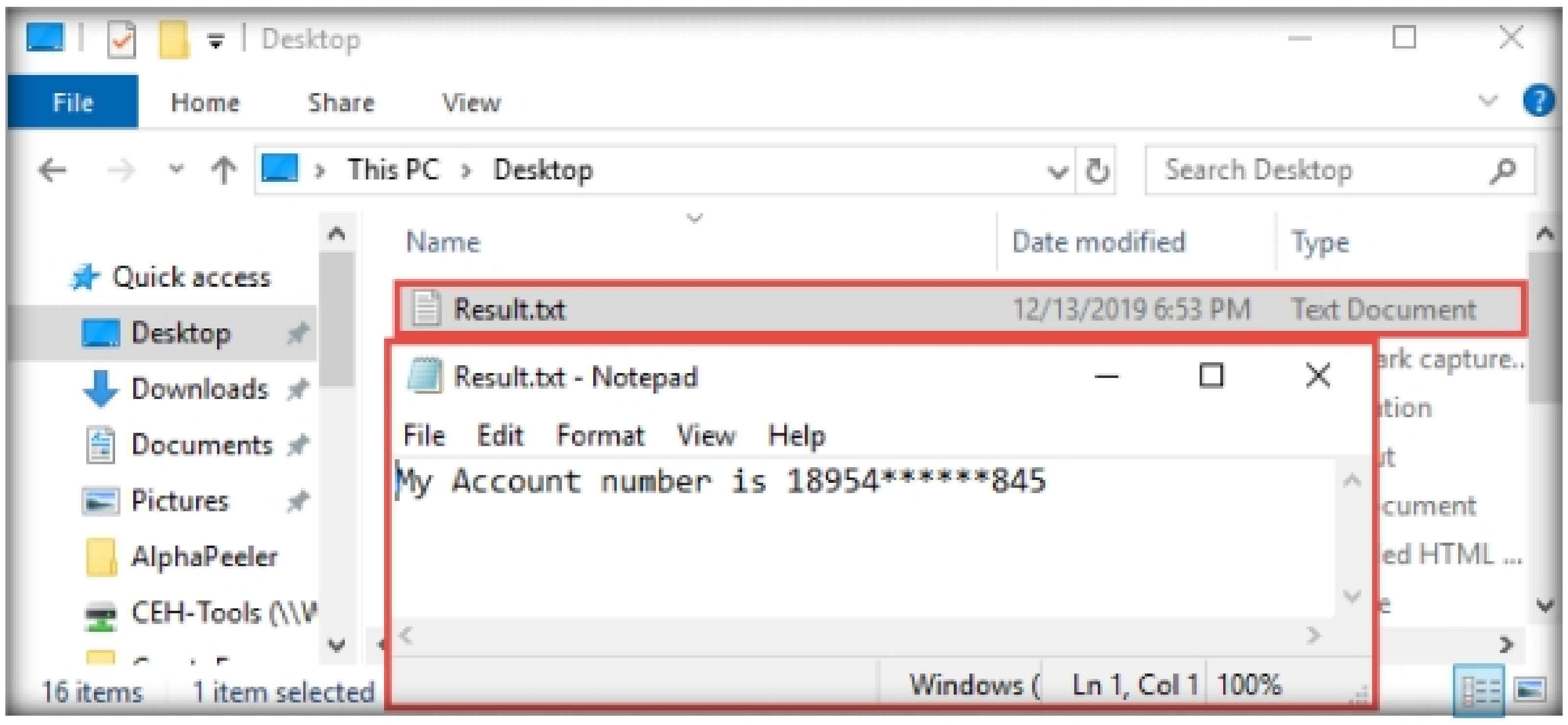
Cipher text file: Z:\CEHv11 Module 20 Cryptogra

Pass phrase: ********

Figure 5.2.16: DES crypto

You can also use other cryptanalysis tools such as **Cryptosense** (https://cryptosense.com), **RsaCtfTool** (https://github.com), **Msieve** (https://sourceforge.net), and **Cryptol** (https://cryptol.net) to perform cryptanalysis.

28. Navigate to **Desktop** and double click the **Result.txt** file. You can observe the file content in plain-text, as shown in the screenshot.


Desktop
File
Home
Share
View
This PC > Desktop
Search Desktop
Quick access
Desktop
Downloads
Documents
Pictures
AlphaPeeler
CEH-Tools (\\V
Name
Date modified
Type
Result.txt
12/13/2019 6:53 PM
Text Document
Result.txt - Notepad
File
Edit
Format
View
Help
Windows (
Ln 1, Col 1
100%
16 items
1 item selected

```
My Account number is 18954******845
```

Figure 5.2.17: Decrypted file

29. This concludes the demonstration of performing cryptanalysis using AlphaPeeler.

30. Close all open windows and document all the acquired information.

31. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

EC-Council

C|EH™
Certified Ethical Hacker

EC-COUNCIL OFFICIAL CURRICULA